Fall 11-5-2021

Intelligent Internet of Things Frameworks for Smart City Safety

Dimitrios Sikeridis
Doctoral Student, Electrical and Computer Engineering

Dimitrios Sikeridis

Candidate

Electrical and Computer Engineering

Department

This dissertation is approved, and it is acceptable in quality and form for publication:

Approved by the Dissertation Committee:

Michael Devetsikiotis , Chairperson

Manel Martinez-Ramon

Ali Bidram

Ioannis Papapanagiotou

I. Safak Bayram

Intelligent Internet of Things Frameworks for Smart City Safety

by

Dimitrios Sikeridis

Diploma, Electrical and Computer Engineering, University of Patras, 2016
M.Sc., Computer Engineering, The University of New Mexico, 2018

DISSERTATION

Submitted in Partial Fulfillment of the
Requirements for the Degree of

Doctor of Philosophy
in Engineering

The University of New Mexico

Albuquerque, New Mexico

December 2021

Dedication

To my parents Stelios and Stavritsa, and my sister Efstratia.

Acknowledgements

First, I would like to deeply thank my advisor Prof. Michael Devetsikiotis for believing in me, and providing the opportunity to further my graduate studies. Prof. Devetsikiotis, I am incredibly grateful for your constant support, mentorship, and encouragement throughout my years of studying.

To my committee — thank you for your time, for your valuable feedback and suggestions on improving this work. Special thanks to Ioannis Papapanagiotou for our collaboration, and his guidance over the years. I also thank Kostas Christidis for working with me, and for his valuable advice.

I was also extremely fortunate to have worked with Panos Kampanakis during my time at Cisco Systems. Thank you for giving me a chance to work on exciting new networking areas. I am grateful to you both for helping me out when I was starting and for your valuable advice and support. Moreover, I am very grateful to my colleagues and friends at VMware, esp. Marc Brotherson, Sean Huntley, and Akeem Jenkins, for their encouragement during my time there.

To Tasos, Greg, Spyros, and all my friends wherever they may be right now — thank you for your continuous encouragement and for making this a ride to remember. To my US brother and sister, Marios and Yana — thank you for all the years we spent together, and your constant support.

Finally, I am extremely grateful to my family for their unconditional love and support over the years. This dissertation would not have been possible without you.

Intelligent Internet of Things Frameworks for Smart City Safety

by

Dimitrios Sikeridis

Diploma, Electrical and Computer Engineering, University of Patras, 2016
M.Sc., Computer Engineering, The University of New Mexico, 2018
Ph.D., Engineering, The University of New Mexico, 2021

Abstract

The emerging Smart City ecosystem consists of a vast edge network of Internet of Things (IoT) devices that continuously interact with mobile devices carried by its citizens. In this setting, the IoT infrastructure, apart from the main communications facilitator, acts as a crowdsourcing mechanism that collects massive amounts of user data, and can support public safety applications for the Smart City. In this thesis, we design and analyze learning mechanisms that extract intelligence from crowd interactions with the wireless IoT infrastructure, and optimize its energy efficiency while operating as a public safety network. First, we deploy a multi-story facility testbed and perform an extensive real-subject trial to gather user interactions with a realistic IoT infrastructure. The resulted BLEBeacon dataset is a collection of Bluetooth Low Energy (BLE) advertisement packets generated from BLE beacons carried by people following their daily routine. To aid fingerprinting localization services, instead of extensive offline measurements, we use the gathered unlabeled Received Signal Strength Indication (RSSI) samples to design a user localization and mobility tracking framework that relies on unsupervised learning.

Following that, we study the transformation of the Smart City's underlying IoT network (edge devices and user equipment) into a Public Safety Networks (PSN) able to provide resilient communications under disaster recovery scenarios. We first propose a heterogeneous device-to-device PSN framework that utilizes reinforcement learning to select the most appropriate wireless protocol, in terms of topology, protocol specifications, and battery-life extension. The framework also utilizes a coalition formation approach that

considers social relations among devices, physical distance,and energy availability. Each device's optimal transmission power is obtained through the formulation of a utility-based power control problem as a non-cooperative, distributed game among IoT devices, that converges to a unique Nash equilibrium. The second PSN framework we propose builds on this power management and combines Unmanned Areal Vehicle (UAV)-support with wireless powered communication (WPC) techniques to further improve energy efficiency. The IoT devices use reinforcement learning to form clusters and actively associate with a cluster-head. Towards extending the PSN's lifetime, we utilize a harvest-transmit-store WPC mechanism, the UAV optimal positioning in the Euclidean 3D space is determined through an optimization problem of maximizing the coalition head's total energy availability.

Finally, we propose an extensive form perfect information game to model interactions and optimal city resource allocations when a Terrorist Organization (TO) performs attacks on multiple targets across two conceptual Smart City (SC) levels, a physical, and a cyber-social. The Smart City Defense Game (SCDG) considers two SC agencies that have to defend their physical or social territories respectively, and fight against a common enemy, the TO. Each layer consists of multiple targets and the attack outcome depends on whether the resources allocated there by the associated agency, exceed or not the TO's. Each player's utility is equal to the number of successfully defended targets. The two agencies are allowed to make budget transfers provided that it is beneficial for both. We completely characterize the Sub-game Perfect Nash Equilibrium (SPNE) of the SCDG that consists of strategies for optimal resource exchanges between SC agencies and accounts for the TO's budget allocation across physical and cyber targets.

Table of Contents

List of Figures

List of Tables

List of Publications

This thesis has resulted in the publication or submission of manuscripts in peer reviewed conferences, journals, and venues. Below, there is a list of this thesis' output ordered by chapter (indicated in bold):

1. D. Sikeridis, "IoT-enabled Knowledge Extraction and Edge Device Sustainability in Smart Cities," 2020 IEEE International Conference on Smart Computing (SMARTCOMP), Bologna, Italy, 2020, pp. 264-265. **(Chapter 1)**

2. D. Sikeridis, I. Papapanagiotou, M. Devetsikiotis, CRAWDAD dataset unm/blebeacon (v. 2019-03-12), download from https://crawdad.org/unm/blebeacon/20190312, Mar 2019. **(Chapter 2)**

3. M. Inaya, M. Meli, D. Sikeridis, and M. Devetsikiotis, "A Real-Subject Evaluation Trial for Location-Aware Smart Buildings", in Conference on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, GA, USA, May 1-4, IEEE 2017. **(Chapter 2)**

4. D. Sikeridis, M. Devetsikiotis, and I. Papapanagiotou, "Occupant Tracking in Smart Facilities: An Experimental Study", In Signal and Information Processing (GlobalSIP), 2017 IEEE Global Conference on, pp. 818-822. IEEE, 2017. **(Chapter 3)**

5. D. Sikeridis, B.P. Rimal, I. Papapanagiotou, and M. Devetsikiotis, "Unsupervised Crowd-Assisted Learning Enabling Location-Aware Facilities", IEEE Internet of Things Journal 5, no. 6 (2018): 4699-4713, 2018. **(Chapter 3)**

6. D. Sikeridis, E. E. Tsiropoulou, M. Devetsikiotis and S. Papavassiliou, "Context-Aware Wireless-Protocol Selection in Heterogeneous Public Safety Networks," in IEEE Transactions on Vehicular Technology, vol. 68, no. 2, pp. 2009-2013, Feb. 2019. **(Chapter 4)**

7. D. Sikeridis, E.E. Tsiropoulou, M. Devetsikiotis, and S. Papavassiliou, "Self-Adaptive Energy Efficient Operation in UAV-assisted Public Safety Networks," in IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), pp. 1-5, June, 2018. **(Chapter 5)**

8. D. Sikeridis, E.E. Tsiropoulou, M. Devetsikiotis, and S. Papavassiliou, "Wireless Powered Public Safety IoT: A UAV-assisted Adaptive-learning Approach towards Energy Efficiency", in Journal of Network and Computer Applications 123 (2018): 69-79. **(Chapter 5)**

9. D. Sikeridis, M. Devetsikiotis, "Smart City Defense Game: Strategic Resource Management during Socio-Cyber-Physical Attacks", submitted. **(Chapter 6)**

In addition, below there is a list of publications that are not directly related to this thesis. They are products of research work in adjacent areas related to the Internet of Things, Smart Cities, Distributed Systems, and Network Security:

10. K. Christidis, D. Sikeridis, Y. Wang, M. Devetsikiotis, "A framework for designing and evaluating realistic blockchain-based local energy markets", in Applied Energy 281 (2021): 115963.

11. D. Sikeridis, A. Bidram, M. Devetsikiotis, and M. Reno, "A Blockchain-Based Mechanism for Secure Data Exchange in Smart Grid Protection Systems", in 2020 17th IEEE Annual Consumer Communications & Networking Conference, IEEE CCNC 2020, pp. 1-6.

12. D. Sikeridis, and M. Devetsikiotis, "Joint Capacity Modeling for Electric Vehicles in V2I-enabled Wireless Charging Highways," in 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Tempe, AZ, USA, 2020, pp. 1-6.

13. D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH", in Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies, ACM, New York, NY, USA, 2020, 149–156.

14. D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Post-Quantum Authentication in TLS 1.3: A Performance Study", in Network and Distributed System Security Symposium 2020 (NDSS 2020), San Diego, CA, USA, 2020.

15. P. Kampanakis, D. Sikeridis, "Two PQ Signature Use-cases: Non-issues, challenges and potential solutions", in ETSI/IQC Quantum Safe Cryptography Workshop, 2019, Seattle, USA, WA, November 5-7, 2019.

16. A. Petropoulos, D. Sikeridis, and T. Antonakopoulos, "Wearable Smart Health Advisors: An IMU-enabled Posture Monitor", in IEEE Consumer Electronics Magazine, vol. 9, no. 5, pp. 20-27, 1 Sept. 2020.

17. A. Petropoulos, D. Sikeridis, and T. Antonakopoulos, "SPoMo: IMU-based Real-time Sitting Posture Monitoring", in 7th IEEE International Conference on Consumer Electronics, Berlin. Germany, Sep. 3-6, 2017.

18. D. Sikeridis, I. Papapanagiotou, B.P. Rimal, and M. Devetsikiotis, 2017. "A Comparative Taxonomy and Survey of Public Cloud Infrastructure Vendors", arXiv preprint arXiv:1710.01476.

19. D. Sikeridis, E.E. Tsiropoulou, M. Devetsikiotis, and S. Papavassiliou, "Socio-spatial Resource Management in Wireless Powered Public Safety Networks," in Military Communications Conference (MILCOM), MILCOM 2018 IEEE, Oct., 2018.

20. D. Sikeridis, E. E. Tsiropoulou, M. Devetsikiotis, and S. Papavassiliou. "Socio-physical Energy-Efficient Operation in the Internet of Multipurpose Things." in 2018 IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE, 2018.

21. D. Sikeridis, E.E. Tsiropoulou, M. Devetsikiotis, and S. Papavassiliou, "Energy-Efficient Orchestration in Wireless Powered Internet of Things Infrastructures ", in IEEE Transactions on Green Communications and Networking, 3(2), pp.317-328, 2018.

List of Abbreviations

GPP: Third Generation Partnership Project

BLE: Bluetooth Low Energy

CH: Cluster Head

CRP: Chinese Restaurant Process

D2D: Device to Device

EM: Expectation Maximization

eNB: Evolved Node B

ICT: Information and Communication Technology

ESA: Emergency Service Agencies

IDD-CRP: Interest-Distance-Dependent Chinese Restaurant Process

IoT: Internet of Things

MG: Minority Game

MQTT: MQ Telemetry Transport

NOMA: Non Orthogonal Multiple Access

QoS: Quality of Service

PSN: Public Safety Network

RSSI: Received Signal Strength Indicator

SC: Smart City

SCDG: Smart City Defense Game

SINR: Signal-to-Interference-plus-Noise Ratio

SM: Social Media

TO: Terrorist Organization

UAV: Unmanned Aerial Vehicle

UE: User Equipment

WET: Wireless Energy Transfer

WIT: Wireless Information Transmission

WNP: Wireless Network Protocol

WPC: Wireless Powered Communications

WSN: Wireless Sensor Network

Chapter 1

Introduction

1.1 Background and Motivation

1.1.1 The Smart City Paradigm

Smart Cities (SC) utilize different technologies and data streams towards making optimal decisions and improve life quality through the employment of different actors. Smart City agencies are using more and more data to optimize their response to critical situations, monitor ongoing events, and ultimately utilize their resources more efficiently [173, 234]. While there is not a single definition for Smart Cities today, the vast majority of projects agree that in essence, a SC utilizes Information and Communication Technology (ICT) to further the efficiency of services and optimize the orchestration of resources. The latest definition by the IEEE IoT Initiative's Smart City Working Group is: *"A Smart City is an urban area that uses technological or non-technological services or products that: enhance the social and ethical well-being of its citizens; provide quality, performance and interactivity of urban services to reduce costs and resource consumption; and increase contact between citizens and government" [132].*

The initial smart city initiatives go as back as 2008 when IBM announced the concept of a "Smarter Planet" [343] with a plan to supply digital services and hardware to interested parties. A case in point is Rio de Janeiro's SC operation center that integrates multiple individual agencies towards optimal disaster response and emergency management [278]. Cisco

has been another example of early industry participation in the development of digital platforms for Smart City use with participation in Kansas City, Barcelona, and Songdo [297]. However, until now the realization of the "Smart City" concept by urban planners and city governments has been relying on plain digitalization and automated solution implementations that often overlook the whole equation's human aspect. The inclusion of those who work and reside in the Smart City (SC) environment into the design process is becoming highly significant especially since currently urban population represents the 55% of the world's population, a number that is expected to reach 68% by 2050 (2.5 billion additional residents by 2050) [324]. Moreover, the explosion of the SC market to $237.6 Billion by 2025 [281] has resulted in the active involvement of not only industry players anymore, but also of standards organizations (e.g., IETF, 3GPP, ETSI, IEEE). Also, more and more municipalities and governments actively participate to discuss and address challenges. Some cases in point include the EU's Smart City Initiative, the EU's Horizon 2020 program (a 77 billion euros innovation initiative), and the UN's United Smart City Initiative [88, 310, 324]. Finally, we are observing multiple contributions from universities, non-profit foundations, state-owned utilities, and private-sector companies that develop disruptive technologies that reconfigure city life in practice. A recent example is the rise of multiple e-hailing startups (Lyft, Uber, GrubHub), that have upended traditional taxi and delivery services, and have made an impressive impact in everyday life [324].

There have been many attempts in identifying the basic components of most smart city undertakings. The authors in [324] identify three layers that have to collaborate to make a city "smart". The first layer includes all the traditional (physical and social infrastructure) of the city and its technology base, namely basic wired and wireless communications, and the extended network of sensors, smart devices, and smartphones. Fig. 1.1 further analyses this first smart city infrastructure layer and its components. The second layer consists of the various smart city applications that have been already developed in multiple smart city prototype ecosystems and will be relevant in the years to come. These applications can be categorized across different domains [324], namely:

- Security: Real-time crime mapping, Gunshot detection, Emergency response optimization, Disaster early-warning systems, Crowd management
- Mobility: Real-time public transit information, Autonomous vehicles, Intelligent

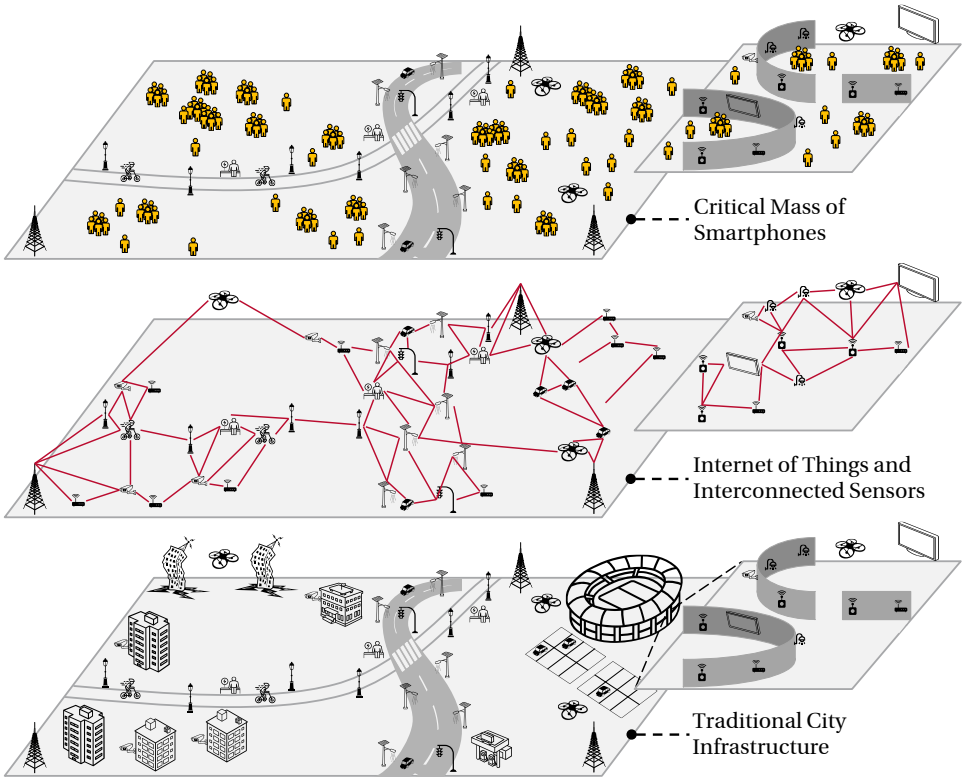


Figure 1.1 Smart City Communication Infrastructure

traffic lights, Smart parking, Bike/Car sharing, E-hailing

- Healthcare: Remote patient monitoring, Telemedicine, Real-time air quality information, Wearables, Infectious disease surveillance, Contact tracing, First aid alerts
- Energy: Home energy automation systems, Dynamic electricity pricing, Distribution automation systems
- Water: Water consumption tracking, Leakage detection, and control, Water quality monitoring
- Waste: Optimization of waste collection routes, Digital tracking for waste disposal
- Economic Development and Housing: Digital business licensing and permitting, Digital business tax filing, Peer-to-peer accommodation platforms

- Engagement and Community: Local civic engagement applications, Digital citizen services

Finally, the third important layer is public adoption of these solutions and broad usage that can lead to behavioral changes.

1.1.2 Internet of Things Integration

Without a doubt, the backbone of any SC undertaking is an Internet of Things (IoT) infrastructure that supports city-wide communications [176, 198, 285, 331] and consists of a vast group of computationally powerful participants including sensors, smart furniture, EVs, drones, 4G/5G eNBs, and WiFi hotspots [14, 148, 167, 261, 280]. The continuously increasing edge IoT network introduces significant challenges that pertain to different aspects of the infrastructure:

1. IoT devices should continuously and seamlessly function with minimal operational cost, making energy efficiency, and battery life very important for the successful large-scale adoption [86, 152].

2. The existence of multiple network protocols and wireless interfaces (WiFi, 4G/5G, Bluetooth, LoRa, NFC, etc.) should be addressed and utilized to collectively aid the availability and connectivity if the massively deployed devices [142].

3. Extra precautions should be taken to enhance the edge network's resiliency in the face of public-safety critical events [255].

Apart from the static IoT infrastructure, modern smart cities are developed around their citizens that carry mobile devices or other User Equipment (UE) with capabilities that far exceed those of the equipment found around cities nowadays. In this setting, the IoT infrastructure is the ideal instrument to conduct mobile crowdsensing which incorporates human intelligence to collect disparate data in pervasive environments [163]. The main characteristics of mobile crowdsourcing in a SC include (i) dynamic mobility of the citizens' UEs that mirror their own, (ii) collaboration, namely the ability of crowds to create social structures and work together to achieve their goals, and (iii) the dual nature of each SC

occupant that is at the same time a data producer, and a consumer as the sensing, communication, and processing of his data enhance the performance of the SC services. Evidently, there are many challenges associated with the above reality that pertains to the efficient design of non-intrusive crowdsensing mechanisms, protection of the SC user's data privacy, and the design of distributed algorithms able to fully exploit the generated data streams in a cooperative and complementary manner for all the offered SC services.

1.1.3 Public Safety Applications in Smart Cities

No community can thrive without basic guarantees of physical safety as it is directly connected to both socioeconomic and psychological markers of urban development [177]. Indeed, according to IHS Markit, the global market for smart city safety lies around 16.2 billion for 2017 and is expected to reach 29.6 billion by 2022 [9]. With that in mind, the effect of Smart City-related technologies (e.g., Internet of Things, cloud computing-based analytics, machine learning) is evident from various prototyping efforts that have been already developed in various cities worldwide. As seen in a McKinsey Global Institute 2018 study [324] the smart application deployment for public safety that was carried out in more than 50 cities affected life quality in a big way. More specifically, the study finds that smart cities that deployed public-safety-related applications accelerated their emergency response times by 2 to 17 minutes through call center optimization (rapid processing and accurate triage), optimization of field operations, preemption of traffic signals, and crowd-sourced critical feeds (text, sound, picture and video submissions by citizens) aiding first responders in accessing emergency scenes. In addition, the study shows a 30 to 40% reduction in crime incidents achieved through passive gunshot detection, video-based threat detection, and crowd-sourced crime alerts that help various security agencies to stay ahead of natural disasters and terrorist threats.

At the same time, however, ensuring public safety in a Smart City environment is an increasingly complicated task due to the involvement of multiple agencies and the city's expansion across cyber and social layers. Indeed, the large critical mass of smartphones, sensors, and IoT devices creates both opportunities for the development of practical applications that ensure public safety and, at the same time, vulnerabilities in terms of privacy, and data security. With that in mind, many public-safety-oriented applications have already

Table 1.1 Examples of Applications that target Public Safety in Smart Cities

Application	**Basic Functionalities**	**References**
Crowd Management	Video/Audio capture and two-way messaging through smart glasses	[301] [193] [302]
Safe Walking Navigation	Minimize transmission latency of security footage through an IoT ecosystem to guarantee safe navigation in walking paths	[218]
Gunshot Detection	Gunshot detection through arrays of acoustic sensors or smartphones	[321] [178] [259]
Motorbike Anti-Theft	Motorbike location and theft detection using an accelerometer, GPS and 3G connectivity	[321]
Critical Communications	UAV-assisted Public Safety Networks	[315]
Contact Tracing	Utilize Bluetooth device-to-device encounters to trace user contact for pandemic response	[196], [30]
Early-Fire Detection and Firefighters' Support	Utilizes smoke and thermal sensors on communication towers for early-fire alarms. Deploys UAVs and IoT connectivity to provide real-time feed to emergency teams for operational planning.	[120]
Flooding Alert	Fusion of crowdsourced and sensor data for early flooding warning and flood mobility detection	[107]

been developed and deployed in smart cities worldwide as city governments are always eager to minimize the toll of natural disasters and black swan events through preparedness and quick response. Table 1.1 summarises representative applications of this nature. In Peru, Telefonica and Honda developed an IoT framework to combat motorbike theft [121].

The design equips each bike with a module that combines 3G connectivity, an accelerometer, and a GPS sensor for theft and real-time location detection. The owners can monitor the position of the bike and receive alerts through a smartphone app. In [218] the authors present a safe walking navigation system where users can utilize surveillance feeds to check current walking paths' safety. Existing communication infrastructure, wireless cameras, and vehicles are used along the information way to process and retransmit the feeds, while the feed's real-time lag is minimized through solving a joint computing resource optimization problem.

Regarding natural disasters, numerous systems aim at early detection towards timely alerting and evacuations [38]. In [107], the authors present a smart flooding alert system that combines data from sensors and crowdsourced feeds to provide real-time alerts during floods, flood-severity level information, and outputs a risk level of flood mobility routes. Similarly, an early-fire detection and support system is presented in [120]. The design utilizes smoke and thermal sensors embedded in communication towers for early-fire detection. In case of a fire, a UAV fleet supported by IoT communications is dispatched to provide a feed of information (use of thermal and optical cameras) to the operations center. The data can be used then for operational planning and firefighters' real-time support. Finally, Japan and Mexico have implemented systems for early warning in case of earthquakes with future additions to include synchronization with elevators (stop and open in case of emergency), shut down of gas pipelines, and alerts to hospitals for timely operating room preparations [324].

Another vector of possible black swan events are attacks from high-level city adversaries like traditional terrorist organizations that have advanced their tactics towards conflicting the maximum possible damage by distributing their forces across multiple city targets. The latest terrorist efforts attest to this observation with the Paris attacks in 2015 taking place simultaneously across six distinct physical locations [138], and the Brussels bombings in 2016 occurring in coordination across two different city targets [296]. In response, some cities including Chicago, London, Beijing, and Singapore have deployed extensive camera monitoring for anomaly detection [324]. Other cities have deployed arrays of acoustic sensors for gunshot detection [178, 259]. In a similar application, the authors in [321] have managed to increase the accuracy of gunshot detection by fusing sensor data from users' smartphones resulting in the possibility of a massive crowdsourced shot detection system

available at any time. Another interesting public safety application that has been reinforced by novel smart city technology is crowd management [47]. City governments are utilizing drones, stationary cameras, and facial recognition to manage crowded events and even scan for possible threats. A case in point is the IoT-based MONICA project [193, 301, 302] that held a real-world where security personnel at a sporting event were equipped with smart glasses. The wearables were able to record video, pictures, audio and transmit the data to the control room monitor in real-time. At the same time, the security personnel could receive messages and alerts from the control room in a visual form [302]. At the same time, this increased use of surveillance tactics raises privacy concerns [104] that has lead to significant design changes of smart city applications that aim to enhance the occupants' privacy [85].

In addition, amidst the era of social media (SM), bad actors are rapidly exploiting technological advancements and trends to improve their tactics [41]. This adaptation creates new city vulnerabilities for exploitation, especially since social media are considered a cyber-social extension of the future SC and during emergencies, people tend to rely more and more on their smartphones. Interestingly, in the last decade, the increasing adaptation of social media by citizens and city agencies during emergencies creates a propagation of information to many directions [241]. This includes citizen to citizen (self-organization, alerting, and aid), SC agencies to citizens (and traditional media to citizens - for public alerting and guidance), and citizens to city agencies (SM integration into monitoring environments for intelligence extraction, situation awareness, and immediate response) [143, 241, 296, 329]. Examples of the massive use of SM during terrorist attacks include the Brussels bombings in 2016 [296], and the Boston Marathon bombings in 2013 [290, 338], where a major concern regarding the credibility of posted information emerged. On the opposite side, the city of Houston after Hurricane Harvey utilized a social-media-shared Google sheet to locate residents in need and create a crowdsourced map for rescue operations with volunteered boats [38]. Therefore, social media (e.g., Waze, Twitter, Facebook) can also create the opportunity for cities to crowdsource data, while some platforms are integrating emergency tools of their own making. Cases in point include Facebook's Safety Check [180], and Airbnb's open house program [6] that utilizes the community's accommodation resources to host people during emergencies, as happened during California's wildfires [87].

Finally, another public-safety-related application family for smart cities is critical communications that create reliable and resilient connectivity environments in disaster-struck areas (natural disasters, terrorist attacks, etc.). Such systems can provide situation awareness, first responder/medical personnel coordination, and smooth adaptation of emergency management protocols. They are usually deployed in dynamic environments with incomplete and uncertain information constraints, degraded or damaged critical infrastructure, and civilian population under panic [266]. In the US, AT&T has been tasked to create, and maintain FirstNet [100], a reliable wireless network dedicated to public safety applications. Since long energy autonomy is critical for such public safety networks (PSN), novel designs are considering airborne platforms as promising solutions for reliable and cost-effective communication in public threatening scenarios. Due to their mobility, unmanned areal vehicles (UAVs) acting as base stations (BS), can approach ground users or target specific UEs leading to lower transmission powers and energy-efficient data aggregation [201, 315]. Additional pros of utilizing UAV-based BSs in PSNs include fast (near real-time) deployment, flexible coverage expansion, and even coverage reestablishment when the existing network infrastructure is not fully operational. Many key vendors are working on projects of deploying airborne BSs for wireless connectivity with Google X's Project Loon (deployed in a disaster response scenario in Puerto Rico [323]), being a case in point.

1.2 Research Objectives and Contributions

Given that (a) the IoT infrastructure will be a critical component of public safety and security services of a future Smart City, (b) within the Smart City this vast edge network of IoT devices coexists and interconnects with mobile devices owned by citizens, and (c) current crowdsourcing mechanisms put user data privacy at significant risk while demanding exhaustive incentive mechanisms, this thesis is ultimately driven by the following research questions:

- How can future Smart Cities utilize wireless interactions of citizens' mobile devices with the existing IoT infrastructure to perform crowdsensing without involving other types of personal data?

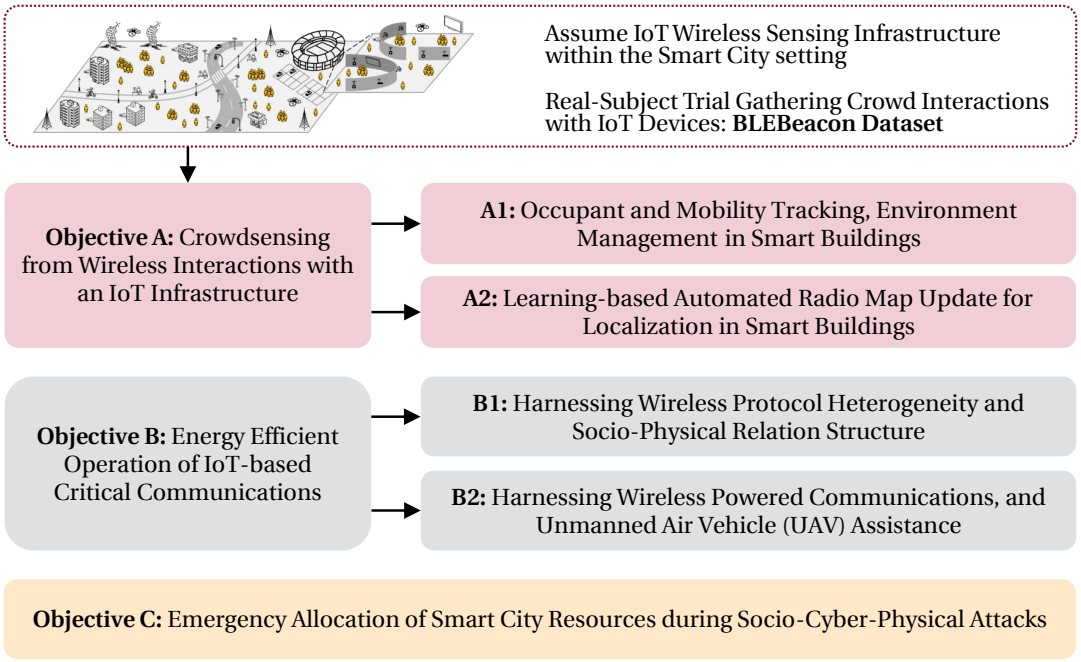


Figure 1.2 Research Objectives

- How can we integrate the same IoT infrastructure into public safety-critical communication networks towards extending their operational lifetime during emergencies?
- How can Smart Cities best allocate emergency resources in the face of a coordinated attack on a cyber-physical level?

Fig.1.2 summarizes the basic research objectives.

In this dissertation, we design and analyze learning mechanisms that rely on an extended IoT infrastructure to support public safety-related services within a Smart City. Our contributions are multifold and are listed below:

1. The first contribution is the BLEBeacon dataset, a collection of Bluetooth Low Energy (BLE) advertisement packets/traces generated from BLE beacons carried by people following their daily routine inside a realistic smart city setting. In more detail, an actual IoT network of Raspberry Pi 3 (RPi)-based edge devices were deployed inside a multi-floor facility continuously gathering BLE advertisement packets. The data were

collected during an IRB (Institutional Review Board for the Protection of Human Subjects in Research) approved one-month-long trial. The focus is on presenting a real-life realization of wireless interactions between smart city residents and an IoT infrastructure, that can provide insights for crowdsensing platforms, public safety applications (e.g., contact tracing), building management, and user-localization frameworks.

2. The second contribution is the design of a passive crowdsourcing framework that supports wireless fingerprinting localization services. To that end, instead of extensive offline measurements, we use passive wireless interactions between users and IoT devices to gather unlabeled Received Signal Strength Indications (RSSI) samples. To support user localization functionality and mobility tracking, we utilize a probabilistic cell-based model coupled with unsupervised and semi-supervised machine learning algorithms. Our approach maintains the positioning accuracy regardless of changes in the underlying hardware or indoor environment.

3. The third contribution is the proposal of a heterogeneous Public Safety Network (PSN) architecture where multiple wireless protocols are utilized to establish resilient peer-to-peer communications during Smart City emergencies. Specifically, commercial user equipment (UE) devices act as learning automata and through a machine learning approach select the most appropriate wireless protocol, in terms of environment/topology needs, protocol specifications, and PSN battery-life extension. Our framework also performs UE clustering through a modified Chinese Restaurant Process – that considers UEs' communication interest (social interest), physical distance, and energy availability –, and obtains each UE's optimal transmission power through a utility-based power control problem to further extend the critical communication network's operation.

4. The fourth contribution is the design of a Public Safety Network architecture that integrates IoT nodes readily available within a Smart City. The proposed framework combines Unmanned Aerial Vehicle (UAV)-support with wireless powered communication (WPC) techniques to further improve energy efficiency in the resulting PSN. The IoT devices form coalitions by initially choosing their role, following the theory of Minority Games (MG). Subsequently, the member nodes act as stochastic learning

automata to associate with a coalition head using a reinforcement learning technique. Towards extending the PSN's lifetime, we utilize a harvest-transmit-store WPC mechanism, where the IoT nodes harvest energy from the mobile UAV before transmitting their information. The UAV optimal positioning in the Euclidean 3D space is determined through an optimization problem of maximizing the coalition head's total energy availability, as these nodes play a critical role within the PSN acting as emergency gateways. Finally, a non-cooperative game-theoretic approach is adopted to determine the optimal uplink transmission power of each IoT node in a distributed manner.

5. Finally, the fifth contribution is the proposal of an extensive form perfect information game to model interactions and optimal city resource allocations when a Terrorist Organization (TO) performs attacks on multiple targets across two conceptual Smart City (SC) levels, a physical, and a cyber-social. The Smart City Defense Game (SCDG) considers three players that initially are entitled to a specific finite budget. Two SC agencies that have to defend their physical or social territories respectively, fight against a common enemy, the TO. Each layer consists of multiple targets and the attack outcome depends on whether the resources allocated there by the associated agency, exceed or not TO's. Each player's utility is equal to the number of successfully defended targets. The two agencies are allowed to make budget transfers provided that it is beneficial for both. We completely characterize the Sub-game Perfect Nash Equilibrium (SPNE) of the SCDG that consists of strategies for optimal emergency resource exchanges between SC agencies and accounts for the TO's budget allocation across the physical and social targets.

1.3 Application Scenario

Although the contributions of this thesis are not application-specific, we use this section to discuss a scenario where our findings and frameworks can be applied.

Let us consider a scenario where Huey is a resident of a future smart city, named Duckburg that has adopted – among others – the frameworks presented in this thesis. Duckburg maintains an operation center that controls (a) all of its agencies (e.g., Duckburg Informa-

tion and Communication (ICT) agency, Duckburg Emergency Service Agency (ESA), etc.) and (b) all of its communication and information infrastructure, and a massive IoT network that consists of IoT devices found in public spaces (i.e., cameras, environmental sensors, smart traffic/street lights, etc.) and IoT nodes within various facilities provided that facility managers have allowed for their IoT equipment to be part of the extended Duckburg IoT network (e.g., with installed Duckburg-maintained software). Also, Duckburg has developed the localization framework discussed in Chapter 3 using its IoT infrastructure which is a city-wide extension of the one we examine in Chapter 2.

Huey always carries his smartphone that has wireless charging capabilities and four wireless protocol interfaces, namely cellular, WiFi, BLE, and NFC. He has also installed the Duckburg Smart City App that among others has access to his smartphone's aforementioned interfaces, has an active beacon operation similar to the one discussed in Chapters 2 and 3, contains an emergency function, and can integrate his device into the Duckburg IoT ecosystem. Huey starts his day by walking out of his house to use the subway to get to his day job. As usually happens, he has not charged his smartphone overnight, and its battery life is at a low percentage. Thus, the Duckburg Smart City App operates its active BLE beacon function in a low frequency, while the Duckburg passive localization system also used ambient tracking from his smartphone (e.g., WiFi probe requests). While at the subway station and inside the train – where GPS localization is not accurate and is complemented by the framework in Chapter 3 –, Huey sits by Alice that also utilizes Duckburg's smart services. Since their smartphones' advertisement packets are simultaneously captured by smart cameras, and the smart lighting within the station and train, their encounter is logged as part of the Duckburg Post-Covid19 [5] Contact Tracing service which operates similarly to the one outlined in Chapter 2.3. If any party is diagnosed with the virus the other will be informed accordingly if the incident happens within a reasonable time-frame. Otherwise, their encounter is deleted.

As Huey arrives at his job facility, he is the first one there. Due to the indoor localization framework, the facility's lighting and temperature are automatically adjusted as he moves towards his office. After some time, his colleagues Dewey, and Louie, that sit beside him, also arrive. At noon they start hearing explosions all over the city. One of them, is just outside their office, where part of their facility collapses, all the exits are sealed with the ruble, and they become trapped. Power is out and the same happens to the cellular connection on

their smartphone as nearby towers are out as well. Immediately, they enable the emergency function on their Duckburg Smart City App. The App attempts to establish a public safety network using peer smartphones and other battery-powered IoT devices and sends a continuous distress signal that can contain text, images, video, and sound to guide first responder operations. Among others, the App contains the framework discussed in Chapter 4 and Chapter 5. Initially, following the heterogeneous PSN operation described in Chapter 4, Huey, Dewey, and Louie's smartphone applications consider protocol specifications, and their topology and choose to operate under BLE while – due to sociophysical characteristics of the available devices (they are physically close and have high communication interest) – create a cluster that consists of these three smartphones. Louie's smartphone is selected as cluster head due to better energy availability and assumes the responsibility to aggregate the data within the cluster and transmit them to a nearby IoT device for further forwarding.

In the meantime, the Duckburg operation center has been continuously receiving multiple streams of critical operational data through the established PSN. They identified a terrorist attack with multiple targets all over the city and activate the emergency smart city resource allocation framework discussed in Chapter 6. After considering the balance between physical and cybersocial (e.g., misinformation campaigns) targets the framework suggests optimal budget exchanges between agencies and allocates different resources to each city target. Since the facility of the three friends is a physical target, and distress signals are being received from their location, the Duckburg operation center dispatches resources there. As first responder units are initially sent to more critical locations (i.e, broader destruction or casualties), the operation center dispatches a UAV to their location to maintain critical communications. When the UAV arrives at Huey' estimated location the Duckburg Smart City App on all smartphones and IoT devices changes its operation to implement the framework presented in Chapter 5. First, the frameworks utilize reinforcement learning to choose new cluster heads and form clusters. The cluster's formation is kept as is, and Dewey's smartphone now becomes the cluster head as the other two devices are low on power (Huey's smartphone all along, and Louie's battery is depleted after acting as an aggregator for a long time). The UAV continuously moves to optimize the charging efficiency for the cluster heads while also wirelessly charging the other devices in the local PSN towards extending its operation lifetime. By doing so all devices use the uplink power management presented in Chapter 5 to continue to transmit critical data – localization

beacon, even voice or video –, and pinpoint Huey, Dewey, and Louie's coordinates while rescue workers try to locate them and extract them, which can take several hours.

1.4 Outline

The rest of the thesis is organized as follows. In Chapter 2, we present the BLEBeacon dataset, a collection of Bluetooth Low Energy (BLE) encounters between people following their daily routine and an IoT infrastructure. Next, in Chapter 3, we present an unsupervised learning framework for passive user localization in an IoT-equipped smart space. In Chapter 4, we focus on extending the battery-life of public safety networks and present a framework that enables them to operate in a heterogeneous fashion utilizing multiple wireless protocols through reinforcement learning. Next, in Chapter 5 we further extend the PSN energy-efficiency during emergencies through a framework that utilizes a mobile UAV able to both aggregate data from multiple IoT devices and charge communication equipment through wireless charging. Following that, in Chapter 6 we propose an extensive form perfect information game to model optimal smart city resource allocations in case of cyber-physical attacks across multiple targets. Finally, in Chapter 7 we conclude the thesis with a summary and a future work discussion.

Chapter 2

The BLEBeacon Dataset

The BLEBeacon dataset is part of the CRAWDAD Community Resource repository [269, 270]. Mahdi Inaya and Michael Meli, from the Department of Electrical & Computer Engineering, North Carolina State University, have contributed to this work. Parts or this chapter were originally published in [144]. The work in this chapter has been supported by an IBM Faculty Award.

2.1 Introduction

Advanced smart infrastructures enable creative ways to enhance life quality and provide information flow towards facility owners, supporting occupant localization services, detection of human mobility for public safety, and enabling facility-occupant interaction applications [144, 265]. The limits are pushed beyond managing temperature, door-locks, and general security, to go as far as reducing energy costs, detecting and building knowledge based on human patterns, and improving the occupant-building interaction.

One of the key features such intelligent facilities should possess is the ability to efficiently track occupants' mobility, either to take real-time actions or use the data to calculate long-time patterns. This type of services is realized either by attempting to estimate the user's 2D coordinates in a given space, which is referred to as micro-location [334, 335], or by attempting to accurately place the user in the vicinity of certain anchor points, known as proximity sensing [337]. Alternative methods that utilize data from body-mounted

Inertial Measurement Units (IMUs) have yielded accurate results concerning microlocation [223],[185]. However, the cost of mass distribution to individuals along with the lack of a central processing and decision-making node (such as a Cloud federation), prohibit their use in well-attended everyday-use environments, making them more appealing to first responder localization applications [340]. Sub-meter accuracy, scalable and low-cost installation, as well as low energy demands, are important factors for large scale indoor localization services.

In this chapter, we introduce and document a dataset of Bluetooth Low Energy (BLE) advertisement readings [137] collected during an IRB-approved one-month trial with real participants. The central component in our approach is a moving BLE beacon architecture that deploys static scanners to intercept advertisement packets. Gathered packets supported two functionalities (see section 2.2.3) and were forwarded to a central server to be used for real-time visualizations, or occupant activity recognition. To the best of our knowledge, this is the first work that provides a dataset extracted from a large-scale multi-floor setting and for an extensive one-month long experiment period.

2.2 BLEBeacon Dataset

2.2.1 Bluetooth Low Energy Beacons

The BLE standard was proposed by the Bluetooth Special Interest Group (SIG) and is designed for low transmission power, short data burst communications. The protocol is operating at the 2.4 GHz frequency band with 40 channels of 2MHz spacing (3 for advertising, 37 for data transmissions). While BLE supports the classic master/slave connection paradigm its extremely energy efficient nature drew attention to a new class of mini-scale devices the BLE beacons. These devices operate by periodically broadcasting packets/identifiers at a specific time interval and transmission power. On the receiving end of those transmissions there can be BLE enabled devices able to utilize information such as the Received Signal Strength Indicator (RSSI) to support various applications with Micro-Location, geofencing [335], and occupant tracking [265] being some cases in point. The sustainability of such a use case is further supported by the low power consumption of BLE beacons that allows the devices to be powered by a coin cell battery for years before any need for reconfiguration.

In light of the above, initially, Apple with iBeacon [110] and later Google with Eddystone [116] standardized BLE beacon protocols (essentially the advertising packet formats). A BLE beacon that utilizes the iBeacon profile transmits a message that contains three pieces of data: (a) A Universally Unique Identifier (UUID) which is the identity of the beacon (b) a Major value that denotes general spatial information, and (c) a Minor value that denotes more specific spatial information. Regarding Eddystone the operation is similar to the iBeacon with the exception that it can support four different payload types in its frame format: (a) Unique ID (UID) frame - denotes identity and consists of two parts Namespace (10 bytes), and Instance (6 bytes) (b) URL address frame (URL) - carries a URL that the BLE end device can directly open (c) Sensor Telemetry frame (TML) - can be used to send sensor data, and (d) Ephemeral Identifier frame - the beacon broadcasts a continuously changing identifier that can be resolved to data by an end BLE device that shares a specific key with the beacon (security feature). More information regarding BLE Beacons and their applications in the Internet of Things settings can be found in [335],[147, 336].

2.2.2 Sensing Infrastructure and Trial

BLE Advertising Devices

Facility occupants carry off-the-shelf BLE-based beacons that continuously transmit BLE advertisement packets. We used the Gimbal Series 10 iBeacon [110, 113] configured to broadcast under the same 16-byte universally unique identifier (UUID). Each beacon is distinguished by a 4-byte identifier inside the manufacturer BLE advertisement packets. The periodic transmission rate for each beacon is set to 1 Hz, with omnidirectional antenna propagation setting, and transmission power of 0 dBm.

Sensing Infrastructure

The deployment of the sensing infrastructure aimed for easy installation and cost-efficiency. Thus, the backbone of the system is the Raspberry Pi 3 (RPi), which can listen to the BLE advertisement channels, and collect all generated packets. All utilized RPi edge devices are connected through WiFi and act as MQTT (Message Queuing Telemetry Transport) [203] clients transmitting information to an MQTT broker hosted by the server. The server per-

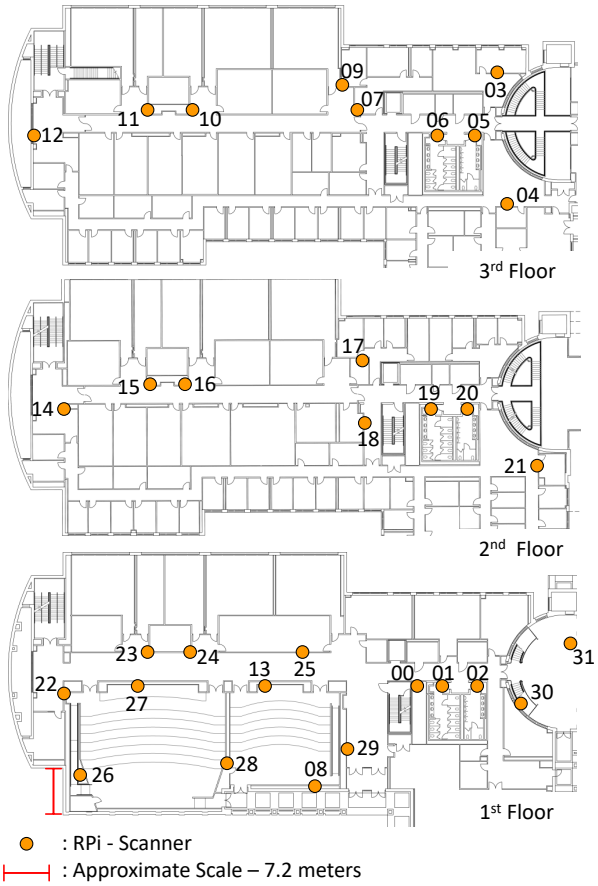


Figure 2.1 Location of RPis - Facility topology

forms data management, validating and storing information in a MariaDB SQL database.

Thirty-two RPis were installed on three floors within NCSU Centennial Campus - Engineering Building II to support the experiment. The exact location of the RPis in the three-floor setting is shown in Fig. 2.1.

Operation

Regarding system operation two approaches were utilized in parallel:

1. *RSSI Report*: all advertisement packet receptions from occupant beacon devices are directly reported to the server with a message that contains the beacon/user ID, the

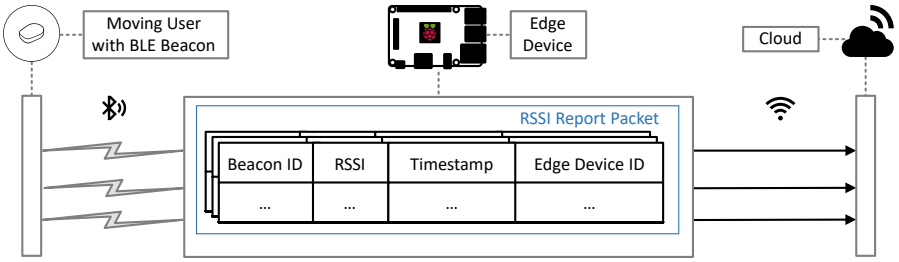


Figure 2.2 RSSI report operation

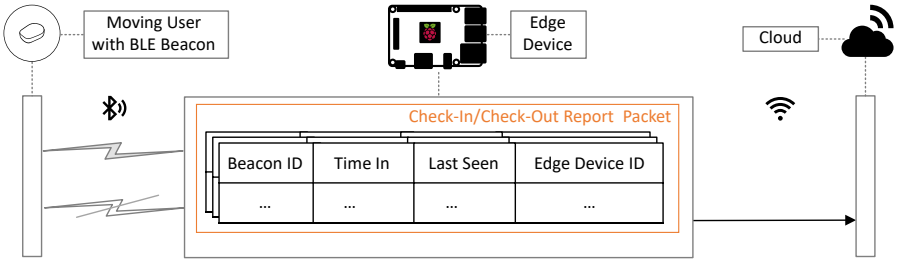


Figure 2.3 Check-In/Check-Out report operation

packet's Received Signal Strength Indicator (RSSI), a reception timestamp, and finally the ID of the RPi that received the advertisement, as seen in Fig. 2.2.

2. *Check-In/Check-Out Report*: each RPi scanner continuously manages a list of current occupants/users in its proximity. A *check in* timestamp is created during occupant's initial entry, and while this beacon is still being detected by the RPi, a *last seen* timestamp is updated. When the beacon is no longer detected (advertisement packets are no longer being received) a Check-In/Check-Out report packet is created and sent to the server containing the beacon/user ID, the *check in* timestamp, the *last seen* timestamp, and finally the ID of the RPi as seen in Fig. 2.3. A thirty-second period is used to ensure that the occupant exited the RPi proximity.

Real-Subject Trial

Following the system architecture described above, an IRB-approved trial with 46 participants took place from September 15 to October 17 of 2016. Participants included frequent occupants of the building that carried a BLE beacon with them at all times during their

Table 2.1 BLEBeacon IRB Trial & Sensing Infrastructure Information

BLE Beacon Type	Gimbal Beacon Series 10
Number of Beacons/Participants	46
BLE Beacon Scanner Type	Raspberry Pi 3
Number of Scanners	32
Number of Floors	3
Trial Dates	09/15/2016 - 10/17/2016

usual routines. The experiment considered all three-floors (see Fig. 2.2) and the core idea was to get insights on repeated occupant behavior and patterns in relation to the facility environment. Table 2.1 summarizes basic trial and sensing infrastructure information.

2.2.3 Dataset Contents

The discussed dataset consists of two files, one containing the trial readings from the RSSI report operation (*RSSI Report* file) and the other from the Check-In/Check-Out report operation (*Check-In Check-Out Report* file). No participant's personal information was kept or made available to retain personal privacy. The *RSSI Report* file contains the following entries:

- *Entry_id*: the unique identifier of a packet in the dataset.
- *Beacon_id*: unique identifier of the occupant/beacon.
- *RSSI*: the Received Signal Strength Indicator (RSSI) in dB.
- *Timestamp*: Date (Month/Day/Year) and Unix time (Hour:Second) of the advertisement packet reception moment from the Rpi.
- *RPi_id*: RPi that received the packet (see Fig. 2.2).

The *Check-In/Check-Out Report* file contains *Entry_id*, *Beacon_id*, and *RPi_id* as described above with the addition of two entries namely:

- *In_time*: Date (Month/Day/Year) and Unix time (Hour:Second) of the moment a user enters the RPi's vicinity and the first advertisement packet is received.
- *Out_time*: Date (Month/Day/Year) and Unix time (Hour:Second) of the last advertisement packet received from the same user by the specific RPi.

Due to the architecture of the sensing infrastructure where several RPi scanners were deployed in close proximity, a single BLE advertisement packet from an occupant/beacon can be received from multiple RPis. This creates multiple entries of the same packet in the database. Such packets are timestamped during the reception moment at the RPi scanner. The RSSI measurements from different RPis whose locations are known can be used to identify a user's exact location inside the facility.

2.2.4 Measurements

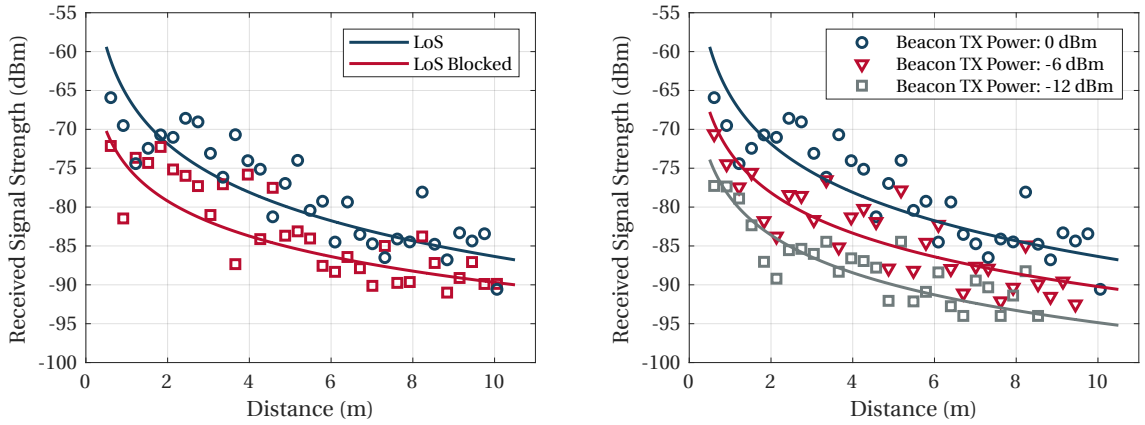
Prior to the full-scale live-subject trial of the system at the ECE department's spaces, we conducted a series of experiments in order to model the received signal strength performance of our configuration as well as examine possible interference events due to RF signal characteristics. Specifically, we estimate the radius covered by each BLE-scanner and examine the possibility of BLE advertisement packets being picked up by scanners positioned on other floors. These measurements characterize in practice the experimental RF environment and are important for any works that plan to utilize the BLEBeacon dataset in the future.

First, we investigate the relation between RSSI and distance. Theoretically, the signal propagation model commonly used to relate RSSI to distance, *d*, is the log-distance path loss model:

$$P_d = P_{d_0} - 10\,\gamma \log(\frac{d}{d_0}) \tag{2.1}$$

where:

- P_d is the RSSI (dBm) at distance d from the source
- P_{d_0} is the RSSI (dBm) at the reference distance d_0 from the source



(a) Line of Sight

(b) 0 dBm beacon TX power

Figure 2.4 Received signal strength vs distance

- γ is the path loss exponent which depends on the propagation channel

Therefore, when unknown, d can be calculated using the expression:

$$d = d_0 \cdot 10^{\frac{P_{d_0} - P_d}{10\gamma}} \tag{2.2}$$

Reference distance d_0 is selected such that it belongs to the antenna's far-field.

The experimental setup consists of a single iBeacon along with a single Raspberry Pi scanner mounted on a hallway wall at the height of approximately 1.6 meters. Measurements were executed at 32 different user-scanner distances varying from 0 to 10.5 meters by averaging all RSSI values received by the scanner over a period of 30 seconds. During the first test, we examined beacon performance in an unobstructed line-of-sight (LoS) between the scanner and beacon, while varying transmission power configurations. Fig. 2.4a shows the RSSI values received at different distances for beacon transmission powers of 0, -6 and -12 dBm. For transmission powers lower than 0 dBm we observed the intermittent loss of advertisement packets after 9 meters, so in order to expand the reach and reliability of an iBeacon BLE packet, we used TX power of 0 dBm for all beacons in the trial.

During the second test, the beacon produced advertising signals at 0 dBm transmission power, while the LoS with the scanner was obstructed by human bodies.Fig. 2.4b shows RSSI values for this test along with a comparison with the case of unobstructed LoS at the

Table 2.2 Floor Bleeding

		Percentage of advertising packets received (%)			
Test	**Test Floor**	**Floor 1**	**Floor 2**	**Floor 3**	**Total Floor Bleeding**
1	1	100.00	0.00	0.00	0.00
2	1	98.74	0.63	0.63	1.26
3	2	2.26	90.94	6.79	9.06
4	2	3.69	91.90	4.41	8.10
5	3	0.00	0.18	99.82	0.18
6	3	0.00	0.91	99.09	0.91
Average		—	—	—	3.25

same TX power level.

In both Fig. 2.4a and Fig. 2.4b, the distance and RSSI measurements were used to perform a curve fitting according to the propagation model described by (2.1). The results demonstrate that the log-distance path loss model is suited to describe BLE signal propagation in indoor environments. This analysis can also be used to determine optimal scanner placement inside a smart building in order to cover all spaces with a minimum beacon transmission power choice.

The second set of experiments were performed by a user equipped with a single iBeacon while moving in the building after all scanners were deployed and fully operational as shown in Fig. 2.1. Test beacons were configured as described in Section III. For each test, a user followed a predefined point-A to a point-B path. In many tests, we examined events where a scanner from another floor picked up the advertisement packet. We refer to these events as floor bleeding events. Table 2.2 shows the results of the aforementioned experiment.

2.3 Public Safety Case Study: Contact Tracing

Recently, smartphone-based contact tracing has emerged as a practical way to trace someone's social exposure with many public-safety-related applications including infectious disease tracking [58]. Such systems can monitor peer to peer interactions between citizens and retroactively provide alerts to users that were in contact with someone that has been diagnosed or tested positive for an infectious disease. A case in point for the importance of such systems is the recent COVID-19 pandemic where many governments have been looking for effective ways to relax restrictions, resume industry operations and bring back daily routines without risking dangerous outbreaks [97]. Therefore, effective contact tracing can be added to the relatively short list of outbreak-preventive measures that also includes regular hand washing, face covering, and temperature checks.

Traditionally, contract tracing is a manual process that requires the collaboration of multiple authorized entities and personnel resulting in a time-consuming operation [84]. Recently, multiple parties have been developing contract tracing applications that rely on peer-to-peer (P2P) architectures that track interactions between individuals through their smartphones or other smart wearables (e.g., smartwatches [214]). The majority of those applications detect either the location or the proximity of two users, and rely mostly on well-known positioning tools that include GPS [130] and more prominently the Bluetooth Low Energy protocol [79, 196, 214, 215, 300]. The logic behind such applications is simple: User devices' transmit and detect BLE advertisement packets, and utilize them to exchange the users' IDs and calculate their proximity. These encounters are logged either on the device or on a remote central authority to be used in case one of the two parties tests positive (in case of infectious diseases) or is picked out for any reason. Then, using history logs other contracts of that person will be identified and alerted either through the device itself or by other means.

While the aforementioned approaches are promising in terms of performance, the overall designs tend to ignore the upcoming reality of a massive internet of things infrastructure already embedded within urban areas and smart cities. Indeed, the proposed BLE advertisement scanning architecture presented in this chapter can lead to the development of an alternative contract tracing application and even reinforce the operation of existing P2P

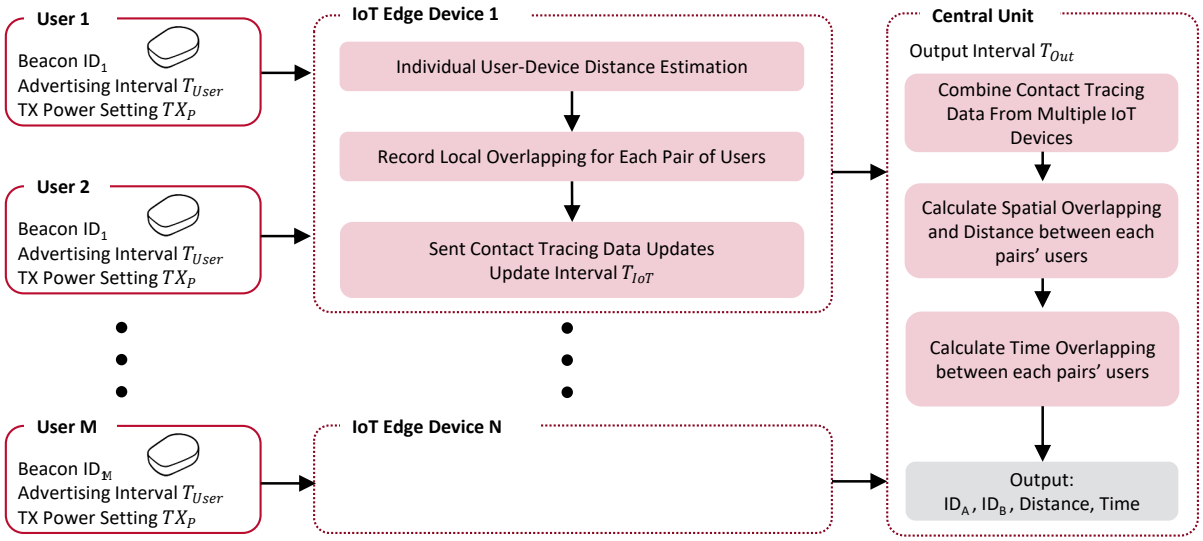
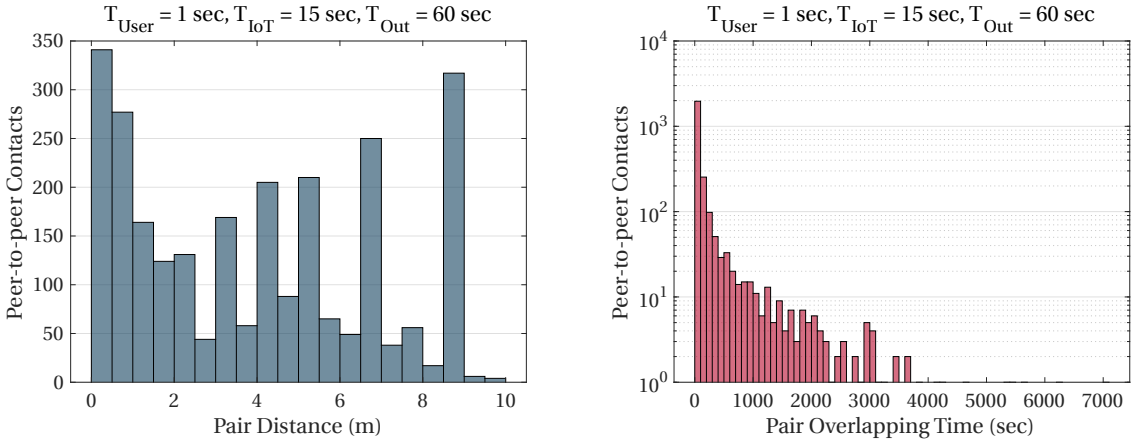


Figure 2.5 IoT-based contact tracing framework using edge devices as anchors

contact tracing and significantly improve their performance and accuracy. In what follows, we present an overview of such IoT-based contact tracing framework and experimentally evaluate the design using the BLEbeacon dataset. Fig. 2.5 outlines the basic operation of the IoT-based contact tracing framework.

The proposed system [7] utilizes the existing IoT devices with multiple wireless interfaces as permanent wireless packet scanners. We will denote as $\mathscr{I}$ the set of $|N|$ IoT devices randomly places in our smart setting (i.e., following the random placement of IoT devices such as cameras, smart locks, sensors, etc.). We will also denote as $\mathscr{U}$ the set of $|M|$ mobile or static users that are frequent occupants on the smart space and carry their respective personal devices. Our design accounts for any kind of personal smart devices, such as smartphone, smartwatch, or other wearables [224, 225], as well as any device with connectivity capabilities handed to the users by the facility/city administrators (e.g., smart id cards). Such devices can emit non-intrusive advertising packets by any of their communication interfaces, with the most common being Bluetooth Low Energy (BLE) advertisement packets (which is the case with the BLEBeacon dataset) and WiFi probe request frames. Our design utilizes such passive user-IoT device interactions to calculate the proximity of a user to an IoT device and document his interaction with other users through the common edge



(a) Number of contacts vs Distance **(b)** Number of contacts vs Duration

Figure 2.6 Contact tracing framework output from BLEBeacon dataset - 09/22/2016-09/29/2016

device with which they are both associated (common anchor). Each personal device can be anonymously linked to its owner from any wireless interface they might utilize for the contact tracing capability. Afterwards, each IoT device reports all the recorded interactions between users to a centralized processing unit that combines information from all sightings and produces a final contact trace between every pair of users. For each pair, our system can calculate the duration of the contact, as well as produce an estimation of the distance between the two users during the contact.

Finally, we evaluate the operation of this contact tracing system using the real-time-generated data from the BLEBeacon dataset. Every entry corresponds to a single interaction between a user and a IoT device. Our analysis considers how our framework would operate during a single week (09/22/2016-09/29/2016). We use an IoT device update period of $T_{IoT} =$ 15 seconds and central unit update interval of $T_{Out} = 60$ seconds and apply the framework to a week-long portion of the BLEBeacn dataset. Fig. 2.6 shows the overall number of contacts against the observed distance, and their overlapping time. The overlapping time results show a strong power law distribution behaviour, which follows previous results on the statistical behaviour of dwell time for human mobility patterns [341].

2.4 Related Work

The majority of existing studies on human activity sensing focus either on restrained settings (small scale) or is employed for a small duration (a couple of days). The work in [44] presents a collection of over 40 million BLE packets coupled with accelerometer and temperature data generated by wristbands of people attending a nightclub. The study duration is two days. The authors in [114] utilize BLE beacon messages to collect proximity data on peer-to-peer interactions in real-life. The study also considers real subjects (6-8 high school students per experiment) and contacts various sessions with different configurations, i.e., standing vs sitting subjects, placement of receiving device on the body, and number of involved subjects. In [194], a BLE RSS dataset is presented focusing on wireless indoor localization as a use-case. The study utilizes a static beacon approach and the measurements were collected in a university setting i.e., an office space, and a library. Finally, the authors in [252] present a dataset containing BLE RSSI readings from mobile users, walking at a constant speed. Again, unlike our work, the beacons are mounted on the ceiling while the BLE packets were collected by wearable smartwatch devices on each user. The aim is to utilize the received RSSI measurements to estimate each user's gait speed.

2.5 Conclusion

This chapter describes the BLEBeacon Dataset, a collection of BLE advertisement packets gathered from a three-floor sensing infrastructure accommodating real-participants carrying iBeacons, following their routines during a one-month period. Possible uses of the dataset include contact tracing, network behavior and reliability detection in similar sensing environments, user mobility pattern extraction due to the experiment's length, occupancy clustering with group identification/monitoring, and provision of facility management or crowd monitoring application insights considering real-life conditions.

Chapter 3

Crowd-assisted Learning for IoT-based Localization

An extended version of this chapter was originally published in [272], while parts of this chapter were originally published in [265]. The work in this chapter was supported by an IBM Faculty Award.

3.1 Introduction

Smart infrastructures are becoming major building blocks of smart cities, able to accommodate a vast variety of services that aim at improving the occupants' routine. More and more of such services are coming to life and equip real-world facilities under the accelerated evolution of the Internet of Things (IoT). Undoubtedly, infrastructures of all sizes and purposes are an ideal environment for organizations and researchers to deploy IoT solutions, where large numbers of edge devices and sensors generate massive amounts of data. The nature of such measurements can be diverse and concern either the occupants (motion, habits) or the building itself (structural health), staging the set of multiple high-quality smart services.

Interestingly, using information extracted by the actual users is an emerging practice nowadays. Crowdsourcing in that sense is becoming a companion of future IoT ecosystems and smart cities, in an uttermost where low-cost tracking of million devices or users is a

vital issue. However, the design of a highly-scalable smart infrastructure to accommodate a large-scale crowdsourcing mechanism is not trivial.

Among various potential services, IoT, in particular, provides an innovative setting for advancing the performance of location-based applications. Accurate indoor localization can be of significance either itself or as a stepping stone in optimizing other services. Smart home management, crowd monitoring in stadiums or sensitive public buildings (e.g., military), navigation or touring in museums [12], and activity monitoring [162, 265], are some cases in point. Many approaches concerning location-based services have been reported. These can be either infrastructure-less solutions that depend on processing signals from inertial measurement units (IMUs) to calculate the location [185], or infrastructure-based solutions that utilize merely wireless protocols (WLAN, Bluetooth, etc.) and their received signal strength indicators (RSSIs) to provide the aforementioned services [91, 118]. Moreover, several attempts try to combine these two approaches with encouraging results [235, 326].

WiFi fingerprinting has been the dominant approach for the received signal strength-based (RSS) localization [25, 118, 322]. Such systems create a massive database of RSS measurements, termed as *fingerprints*, between wireless devices and access points sampling the indoor area. By comparing new fingerprints to the database they can estimate the requested location. At the same time, indoor localization approaches that utilize wireless beaconing are getting popular by improving the accuracy, and energy requirements in a cost-effective way [91, 337]. Recently, the use of Bluetooth Low Energy (BLE) beacons has been actively investigated by both academia (e.g., [12, 91, 162, 265, 337]) and industry (e.g., Estimote, Gimbal, Apple [20]).

In both cases, the fingerprint database can either be deterministically containing raw RSS readings or used to form RSS distribution models leading to probabilistic location estimations. An interesting question that arises concerns the RSS measurement collection practices. Usually, this is performed offline and beforehand leading to a labor-intensive process since wireless channels in indoor environments are extremely dynamic and hard to model [254]. It is a sizable cost since the procedure should be repeated after landscape modifications or changes concerning the wireless equipment. This site-survey offline fingerprint procedure is the main obstacle before widespread adoption and real installation of such systems in future smart facilities.

Lately, crowdsensing has come to the rescue allowing labor-free construction of radio maps by collecting measurements from the users themselves either in the opportunistic or participatory sense [123, 151, 197]. Apart from that, this approach can lead to a continuous and massive collection of measurements that set the stage for utilizing machine learning methods as widely applied lately in wireless communications. Especially in this dynamic RF environment, the ability to train and retrain localization models can actively improve the system's prediction capabilities.

Motivated by the advantages offered by the seamless integration of machine learning and crowdsourcing in indoor positioning applications, this chapter aims to design a three-layer *location-aware* infrastructure. The focus is on creating a smart space for IoT-inspired localization applications, and a low-cost, robust crowdsourcing system where thousands of clients will provide data from a sensing layer towards a cloud-based decision system. Our architecture equips occupants with active beacons, while edge devices are tasked with collecting the generated transmissions. The positioning estimation part is implemented through a cell-based probabilistic model that classifies facility occupants to possible locations.

In order to provide an effortless way to collect RSS fingerprints and train the aforementioned model, we propose an unsupervised learning black-box approach. This logic differs from manual calibration processes that have to be repeated due to environmental changes or landscape reforms, especially in large facilities (e.g., stadium, business complex). Further, the performance of the proposed solution is thoroughly evaluated with different deployment scenarios including different training approaches, adjustable training set, and the size of the decision window.

For the evaluation purposes, we utilized unlabeled samples/fingerprints that were collected during a real-world trial and from real participants on multiple days. This experimental setup makes our system an actual crowdsensing attempt and enables us to test how the learning procedure evolves over time. We also discuss the performance of our setting under a semi-supervised learning approach where a mixed set of labeled and unlabeled samples is used for the training process. Finally, we discuss the ability to track user mobility and the impact of the different installation scenarios (dense and sparse) in facilities with a fluctuating number of visitors.

The main contributions of this chapter are summarized as follows:

- We present the design of a three-tier infrastructure that relies on edge computing and centralized cloud and offers positioning services by utilizing a comprehensive cell-based probabilistic localization model. Moreover, the introduced setting can act as a massive indoor crowdsensing mechanism.
- We propose a black-box approach with a learning algorithm that utilizes unlabeled RSS samples from the actual occupants, making the localization accuracy resilient to indoor environmental changes.
- We deployed an experimental testbed on a multi-story university building and collected data via an IRB-approved trial with real participants. The experiment spanned across multiple days and the collected dataset was used to actively evaluate our concept.

The remainder of the chapter is structured as follows: System model and location-aware architecture are described in Section 3.2. Section 3.3 presents the training algorithm. The experimental setup is detailed in Section 3.4. Sections 3.5 presents the evaluation results, discusses the ability of our system to track user mobility and presents a comparative analysis. Section 3.6 gives insights into deployment considerations, while Section 3.7 discussed the advantages of our approach. Finally, related work is discussed in Section 3.8 and Section 3.9 concludes the chapter.

3.2 System Model

In this section, we describe the location-aware smart facility architecture and the probabilistic localization model along with its underlying assumptions.

3.2.1 Location-Aware Architecture

Our smart space model equips users with beacon-based sensors and utilizes small-factor edge devices to discretize the facility area into a grid of N non-overlapping square $n \times n$ cells as depicted in Fig. 3.1. The discretization can have a non-uniform structure, while ideally, each edge device is placed at the center of the covering cell with its location presumed

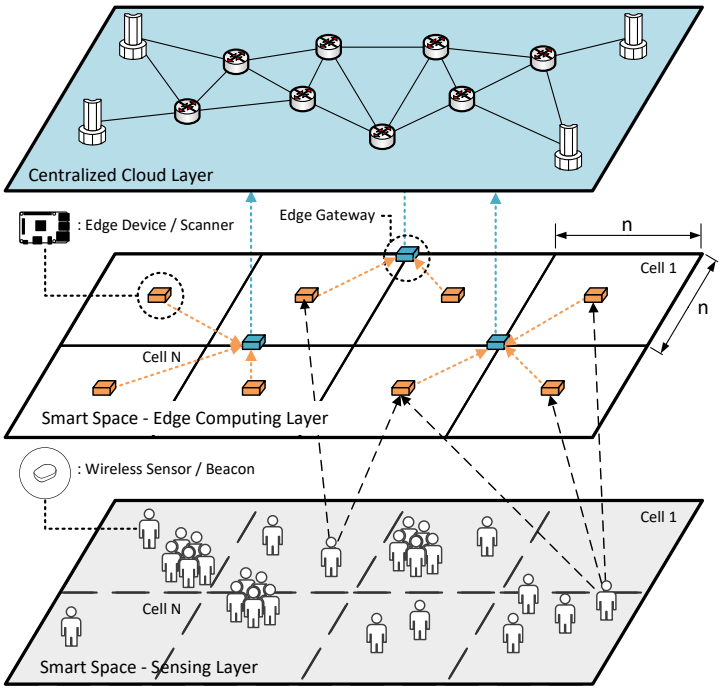


Figure 3.1 Location-aware infrastructure model

known. In terms of the cell area, the model is scalable and configurable to meet any indoor facility needs. Cell dimensions can vary with sides n equal to a couple of meters (for dense space discretization and precise micro-location applications [335]) to tens of meters (for sparse deployments in large facilities and applications related to proximity sensing or crowd monitoring).

Regarding the smart space visitors, they are equipped with RF-beacon devices that periodically broadcast packets at the same transmission power. These packets, that fingerprint the user's location, are being received by one or multiple edge devices in the edge computing layer before being forwarded to a cloud-based centralized decision system (Fig. 3.1). The periodic sampling of a single user's packet received signal strength measurements, can generate a vector of RSSI values sniffed from at a set of different edge devices. Given this vector, the controlling central system periodically - we will refer to this period as *estimation window* or *decision period* - classifies each visitor to the most likely smart space cell.

In our model, the number of scanning devices N equals the number of possible cell locations. Essentially, this is a limitation of our model where each edge device is in charge

of covering a certain square area as depicted in Fig. 3.1. In cases where installed devices, due to physical limitations, have close proximity (see Section 3.4 and Fig. 3.3 with our experimental setup), multiple devices can exist inside the same cell. However, same-cell devices in the specific model will be considered as a single virtual edge scanner, where the RSSIs from each physical device will be averaged (see Section 3.4). Thus, that way any given installation is able to uphold the original model formulation where the number of virtual scanning probes N and the number of cells are equal. Also, for such cases, we are able to limit the database size and achieve more efficient computation.

At this point, we want to discuss the fundamental limitation in machine learning models, which is the tradeoff between how accurately our model can explain the training data vs. the utilized model complexity. The ultimate goal is for our own model to perform well in the case of previously unseen information (here data generated during new days of operation). In light of the above, models of high complexity can fit well almost any training dataset leading to poor performance for diverse input classification data. In comparison, simplistic models perform poorly in fitting test training data, exporting underfitted model parameters. Our focus lies with a balanced attempt at a relatively simple model design that takes into account the practical nature of our deployment.

3.2.2 Probabilistic Model and Assumptions

Given the described system architecture, let C be a discrete random variable that represents the unique N smart space cells. Each cell is expressed by a value $c \in \{1, ..., N\}$ and for the random variable C we define π_c as the a priori probability that the user is at cell c. The corresponding probability mass function (pmf) of C is defined as follows:

$$p_c(C = c) \equiv \pi_c, \;\; 0 \leq \pi_c \leq 1, \;\; \text{and} \;\; \sum_{c=1}^{N} \pi_c = 1. \tag{3.1}$$

In addition, conditioned on the event that the user is located at cell c, we define an N-dimensional random vector $\mathbf{S}_{RSS} = (S_1, ..., S_N)$ that represents the average RSSI values of the user-generated packets received by each one of the $j \in \{1, ..., N\}$ edge devices during an estimation window. The random vector takes values $\mathbf{s} = (s_1, ..., s_j, ..., s_N)$ where s_j expresses the 1-D value of average RSSI in each scanning device. At this point, we will be making two

assumptions regarding the random vector $\mathbf{S}_{RSS}$.

First, we assume that the average RSSI at a given edge scanner - calculated from packets transmitted from a single user located at cell c - follows a Gaussian distribution. This Gaussian assumption is widely used in RF-signal models of both outdoor cellular networks [53] and indoor WiFi settings [118]. To validate this assumption, we collected RSSI samples observed at a single edge device in our BLE-based implementation.Fig. 3.2 shows the pdf and cdf of the resulted RSSI distribution, that portray a strong Gaussian behavior. This hypothesis leads to the production of simple models and contributes to retaining an important tradeoff in machine learning approaches between the best fit on the training data and the resulting model complexity [205].

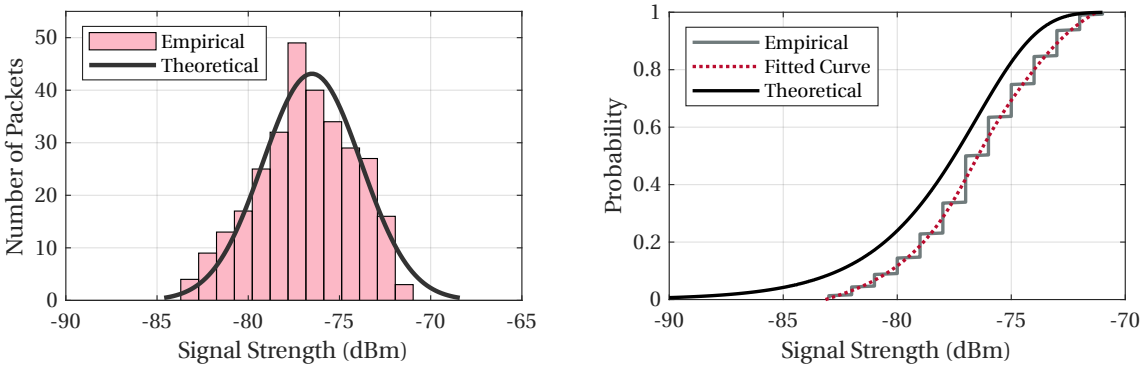
Second, we assume that for the given cell location c of the user, the RSSI values we observe at the different edge devices are conditionally independent (naive Bayes assumption). This assumption is frequently used, e.g., [53, 118] as edge devices are separately located and the wireless channel path losses can be assumed conditionally independent in general. Apart from that, this addition further simplifies the model reducing the number of active parameters and leading to a classifier with stronger resilience to overfitting [205]. Also, it is widely accepted in similar machine learning applications that Bayesian classifiers can produce highly accurate results even when this assumption is violated [78]. In our case, such violations can occur due to user mobility, general placement of the scanning devices, and the physical terrain.

By taking into account the aforementioned assumptions, random vector $\mathbf{S_{RSS}}$ is modeled as an N-dimensional Gaussian random vector with N-dimensional mean μ_c and $N \times N$ covariance matrix Σ_c. The covariance matrix can be further simplified due to the Bayesian assumption to $\sigma^2_{jc} I$ with I being an $N \times N$ identity matrix. Overall, the conditional pdf of $\mathbf{S_{RSS}}$ (likelihood) can be written as follows:

$$p(\mathbf{S} = \mathbf{s} | C = c) = \prod_{j=1}^{N} \mathcal{N}(s_j | \mu_{jc}, \sigma^2_{jc}) \tag{3.2}$$

with:

- $\mathcal{N}(s_j | \mu_{jc}, \sigma^2_{jc}) = \frac{1}{\sqrt{2\pi}\sigma_{jc}} exp(\frac{-(s_j - \mu_{jc})^2}{2\sigma^2_{jc}})$, the 1-D PDF



(a) Gaussian pdf fit

(b) Gaussian cdf fit

Figure 3.2 Gaussian assumption validation - Distribution of RSSI values produced by a single user and received at a single edge device.

- μ_{jc}, the mean RSSI value of packets received at the edge device j with origin point a user at cell c
- σ_{jc}, the corresponding conditional variance of the above

Further, the joint probability function of our localization model is defined as follows:

$$p(C=c,\mathbf{S}=\mathbf{s}) = p_c(C=c)p(\mathbf{S}=\mathbf{s}|C=c) = \\ = \pi_c \prod_{j=1}^{N} \mathcal{N}(s_j|\mu_{jc},\sigma^2_{jc}). \tag{3.3}$$

Finally, given that we model C to be a latent (unobserved) random variable, the marginal pdf of $\mathbf{S}$ will result to a linear superposition of independent Gaussians that constitute a finite naive Bayes Gaussian mixture model (GMM):

$$p(\mathbf{S}=\mathbf{s}) = \sum_{c=1}^{N} p_c(C=c)p(\mathbf{S}=\mathbf{s}|C=c) = \\ = \sum_{c=1}^{N} \pi_c \mathcal{N}(\mathbf{s}|\boldsymbol{\mu}_c,\boldsymbol{\sigma}^2_c) = \sum_{c=1}^{N} \pi_c \prod_{j=1}^{N} \mathcal{N}(s_j|\mu_{jc},\sigma^2_{jc}) \tag{3.4}$$

where we define the final parameters of the resulting model as $\boldsymbol{\theta} = (\boldsymbol{\pi}, \boldsymbol{\mu}, \boldsymbol{\sigma^2})$ with $\boldsymbol{\mu}$ and

$\boldsymbol{\sigma^2}$ corresponding to all conditional means and variances while $\boldsymbol{\pi}$ represents the vector of prior probabilities expressing user existence in each cell.

3.2.3 Cell Estimation

After learning the $\boldsymbol{\theta}$ parameters, a vector $\mathbf{s}$ of observed RSSI values at the edge devices can be given as a real time input to our classifier. The user's location C is designated as the cell c that produces the highest conditional probability calculated by the probability mass function (posterior probability):

$$p(C = c|\mathbf{S} = \mathbf{s}, \boldsymbol{\theta}) = \frac{\pi_c \prod_{j=1}^{N} \mathcal{N}(s_j|\mu_{jc}, \sigma^2_{jc})}{\sum_{\hat{c}=1}^{N} \pi_{\hat{c}} \prod_{j=1}^{N} \mathcal{N}(s_j|\mu_{j\hat{c}}, \sigma^2_{j\hat{c}})}. \tag{3.5}$$

3.3 Model Training

The model parameters are calculated using the powerful Expectation-Maximization (EM) algorithm [75], as frequently applied in machine learning to fit finite GMMs. In this section, we describe training practices and discuss our crowdsourced unsupervised learning approach.

3.3.1 Training Approaches

Our training procedure requires a number of training samples, which is a data set of RSSI observations, namely a data set in the form of the random variable S_{RSS}. To clarify this, let us assume that the training set $\boldsymbol{T}$ consists of K samples indexed using the k symbol, $\boldsymbol{T} = (\boldsymbol{s}^{(1)}, ..., \boldsymbol{s}^{(k)}, ..., \boldsymbol{s}^{(K)})$, where again $\boldsymbol{s}^{(k)} = (s_1^{(k)}, ..., s_j^{(k)}, ..., s_N^{(k)})$ are the RSSI values observed at each one of the N edge devices.

Depending on how these samples were collected they can be either labeled or unlabeled. Labeled sample collection requires a test transmitter located at a known cell c. By observing the RSSI values of the transmissions in each edge device, we can construct the $\boldsymbol{s}^{(k)}$ vector and denote the associated label $c^{(k)} = c$. Thus, the training sample set will be accompanied by a parallel set of labels $\boldsymbol{L} = (c^{(1)}, ..., c^{(k)}, ..., c^{(K)})$, with $c^{(k)} \in \{1, ..., N\}$.

The existence or not of a label set defines the learning approach we can follow:

- *Supervised learning setting*: A complete label set L is available to train the EM algorithm. This approach (discussed in [118]) requires off-line measurements across the entire facility.
- *Unsupervised learning setting*: There is no label set available and unlabeled samples are exclusively used to train the model [99].
- *Semi-supervised learning setting*: A partially complete label set is available. Model training is achieved using both labeled and unlabeled samples [53].

In this work, we propose and examine the possibility of a totally unsupervised training setting, where instead of extensive fingerprint-based offline measurements, we use the facility occupants to gather our training samples. Since the infrastructure is able to collect RSSI measurements from each user, we can utilize this set of observations to train our GMM and identify the connection between occupancy in a cell c and the corresponding RSSI sample s (essentially performing clustering of the training set).

3.3.2 Identifiability and Initialization

A well-discussed issue in training the EM algorithm using this unsupervised approach with unlabeled samples (hidden-latent) is identifiability [53, 205]. Since no labels are offered for the training samples, the combined Gaussian distribution of the RSSIs is not sufficient to associate a sample with a single cell. Namely, the classifier has not enough information to make a connection between the cell label and the actual cell, since for any relabeling of the c index the log-likelihood $\log(p(\boldsymbol{S}=\boldsymbol{s}|\boldsymbol{\theta}))=\sum_{k=1}^{K}\log(\sum_{c=1}^{N}\pi_c\ \mathcal{N}(\mathbf{s}|\boldsymbol{\mu}_c,\boldsymbol{\sigma}_c^2))$ would remain unchanged. Therefore the classifier will be unable to distinguish the N cells from the N! possible label permutations as all of them will give the same solutions [74].

In our case, we have to initially guide the EM algorithm to establish the appropriate connections between the actual (physical) and virtual cell in order to confront the identifiability problem. To achieve that, we have to properly initialize the model parameters $\boldsymbol{\theta}=(\boldsymbol{\pi},\boldsymbol{\mu},\boldsymbol{\sigma^2})$ by relying on real-world observations of the classifying pair, that in our case consists of the user cell location c and the random vector of RSSI readings at the neighboring scanners.

The a priori probabilities π of occupancy in a cell, are initialized uniformly over the N locations of the model. Regarding the other two initialization parameters, there are two ways of extracting them:

- *Wireless channel modeling:* It involves the use of signal propagation models to estimate the path loss between a given cell and the edge device. In this case, model choices can vary depending on the indoor environment and the desired accuracy [254]. After the model construction, one can use the distance between a scanner and a user (possibly located at the center of a cell), to calculate the theoretical RSSI path loss and use it for initializing the mean values $\boldsymbol{\mu}$. Regarding $\boldsymbol{\sigma^2}$, we can use the variance of the experimental measurements that built the model, while the arbitrary choice of a fixed initial $\boldsymbol{\sigma^2}$ has also been reported in [118].

- *War-Walking:* It involves a test beacon device positioned sequentially in every cell, while the scanners record the RSSIs. Following that, the observations in each scanner are used to extract the means and variances $(\boldsymbol{\mu}, \boldsymbol{\sigma^2})$ that initialize the EM. This method, although demanding in terms of implementation can provide superior initial parameters as the test device can be placed at multiple positions inside the same cell yielding better estimates for $\boldsymbol{\mu}$ and $\boldsymbol{\sigma^2}$ -in comparison with extracting all the samples from the cell center. Finally, even if the test device covers only a subset of cells, the mean of the rest can be estimated through spatial interpolation [53].

Since our design attempts a completely unsupervised and effortless deployment, we followed the wireless channel modeling initialization, analytically presented in Section IV-B.

3.3.3 Expectation Maximization (EM) Algorithm

In this Section, we present an overview of the EM algorithm [75], which is modified for supervised, semi-supervised and unsupervised training setting. Input parameters include the aforementioned training set $\boldsymbol{T} = (\boldsymbol{s}^{(1)}, ..., \boldsymbol{s}^{(k)}, ..., \boldsymbol{s}^{(K)})$ and the label set $\boldsymbol{L} = (c^{(1)}, ..., c^{(k)}, ..., c^{(K)})$ that can be complete, semi-complete or empty.

The EM algorithm consists of two main iterative steps that follow the initialization. The Expectation step (E-step), where we fix the model parameters $\boldsymbol{\theta}$ and use each sample $\boldsymbol{s}^{(k)}$ to

Algorithm 1 : Expectation Maximization (EM)

Input: $\boldsymbol{T} = (\boldsymbol{s}^{(1)}, ..., \boldsymbol{s}^{(K)})$, $\boldsymbol{L} = (c^{(1)}, ..., c^{(K)})$, $\boldsymbol{\theta}[t=1]$
Output: $\boldsymbol{\theta} = (\boldsymbol{\pi}, \boldsymbol{\mu}, \boldsymbol{\sigma^2})$
Initialization : $\boldsymbol{\theta}[t=1] = (\boldsymbol{\pi}^1, \boldsymbol{\mu}^1, (\boldsymbol{\sigma^2})^1)$
while not converged **do**
(a) **Expectation (E) step:**
for each k in $\boldsymbol{T}, \boldsymbol{L}$ and each cell c **do**

$$\gamma_{(k,c)} = \begin{cases} p(C = c | \mathbf{S} = \boldsymbol{s}^{(k)}, \boldsymbol{\theta}[t]), & \text{if } c^{(k)} = \emptyset \\ 1, & \text{if } \boldsymbol{s}^{(k)} \text{ is labeled and } c^{(k)} = c \\ 0, & \text{if } \boldsymbol{s}^{(k)} \text{ is labeled and } c^{(k)} \neq c \end{cases}$$

end for
(b) **Maximization (M) step:**

$$\Gamma_c = \sum_{k=1}^{K} \gamma_{(k,c)}, \quad \pi_c^{[t+1]} = \frac{\Gamma_c}{K},$$

$$\mu_{jc}^{[t+1]} = \frac{1}{\Gamma_c} \sum_{k=1}^{K} \gamma_{(k,c)}\, s_j^{(k)},$$

$$(\sigma_{jc}^2)^{[t+1]} = \frac{1}{\Gamma_c} \sum_{k=1}^{K} \gamma_{(k,c)}\, (s_j^{(k)} - \mu_{jc}^{[t+1]})^2$$

$$\boldsymbol{\theta}^{[t+1]} = (\boldsymbol{\pi}^{[t+1]}, \boldsymbol{\mu}^{[t+1]}, (\boldsymbol{\sigma^2})^{[t+1]})$$

end while

calculate the posterior probabilities referred to as responsibilities $\gamma_{(k,c)}$ of component c for the sample k. This procedure is immediately followed by the Maximization step (M-step) where we fix the distribution over the missing labels and compute the model parameters $\boldsymbol{\theta}$ that maximize the expected log-likelihood of the samples. The algorithm proceeds with the E-step alternating with the M-step until convergence to a (local) maximum-likelihood estimation. Algorithm 1 describes the EM process in detail. Index symbol t denotes general algorithm steps with $\boldsymbol{\theta}[t=1] = (\boldsymbol{\pi}^1, \boldsymbol{\mu}^1, (\boldsymbol{\sigma^2})^1)$ being the product of the initialization.

The time complexity of the general EM algorithm depends on the applied structure of the problem. In our case, we examine an N-dimensional Gaussian mixture model with equivalent $|N|$ number of mixtures ($|N|$ different cells/locations) and consider $|K|$ conditionally independent observations/learning samples. Therefore, the computation complexity of the above procedure is proportional to the number of observations $|K|$ and locations $|N|$, for each iteration cycle, which is dictated by the convergence criterion. Specifically, the

computational complexity is $O(|N|(|K|+|K|^2))$ [60]. The aforementioned repetition of E and M steps produces a monotonically increasing likelihood or log-likelihood sequence until a saddle point is approached. The log-likelihood of the $|K|$ observed measurements is calculated as

$$\log(p(\boldsymbol{S}=\boldsymbol{s}|\boldsymbol{\theta}))=\sum_{k=1}^{K}\log(\sum_{c=1}^{N}\pi_c\ \mathcal{N}(\mathbf{s}|\boldsymbol{\mu}_c,\boldsymbol{\sigma}_c^2)) \tag{3.6}$$

The algorithm, in general, converges when changes in the log-likelihood between successive repetitions are less than a predefined threshold. For our implementation, the convergence criterion is met when the log of posterior probabilities exhibit changes under 1%. A detailed convergence analysis of the EM algorithm for Gaussian mixtures can be found in [328]. Since a user's location at any time is provided via equation (5), given the converged trained model, the existence of multiple users does not affect the runtime performance of the system.

3.4 Experimental Setup

Up to this point, we have abstracted the location-aware facility model description from specific wireless communication technology, protocol, or hardware. In this section, we describe in detail our system setup, with emphasis on how this setting enabled the realization of a large-scale experimental testbed with real participants.

3.4.1 System Setup and Real-Subject Trial

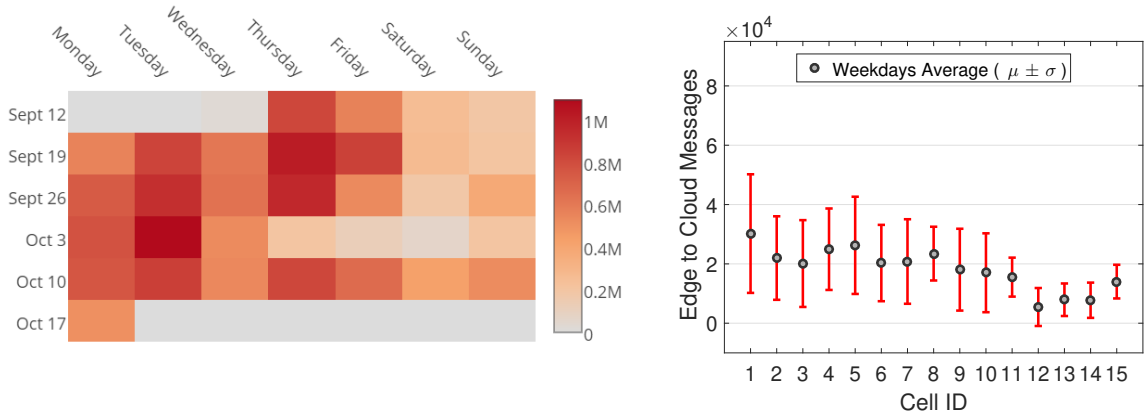
For our case study, we used the experimental setup that was described in chapter 2. Specifically, the utilized testbed was realized on the three-floor setting located at the spaces of North Carolina State University's ECE Dept. Building [144, 264]. The deployment utilized the Bluetooth Low Energy (BLE) as the primary short-range communication protocol. The edge computing layer (see Fig. 3.1), consists of Raspberry Pi 3-based edge devices, able to continuously collect BLE advertisement packets transmitted by occupant's BLE beacons. The exact spatial installation is depicted in Fig. 3.3, and is approximately equal to 2300 m^2 for floor 1, and 1400 m^2 for floors 2 and 3 respectively. The area of each virtual cell shown in Fig. 3.3 is 324 m^2 while if we consider cells that cover dead areas (walls, outside spaces)

Figure 3.3 Smart space topology: Edge device and cell locations.

or partially cover rooms where the existence of occupants is possible we can report that a minimum area is equal to 192 m^2, while a maximum cell area is equal to 450 m^2. Regarding the installation of edge devices, they were placed in different heights, either attached to walls or in the ceiling, as dictated by the existence of power outlets. The minimum installation height for our devices is 0.62m (near floor placement), while the maximum installation height approximately reaches the 2.5m (ceiling installation). Note that this installation is an ideal simulation for actual IoT devices that will be placed randomly (both in location and height) within a Smart City setting.

Regarding the edge layer operation, for each received BLE packet the scanning device acts as a Message Queue Telemetry Transport (MQTT [203]) client, by forwarding an MQTT message through the edge gateway to the centralized cloud layer. Each message contains the edge device ID, the user/beacon ID, the RSSI value of the received packet, and a detailed timestamp of the event.

The smart space environment is completed by occupants carrying Gimbal Series 10 iBeacons [20] that broadcast BLE advertisement packets with 0 dBm transmission power and 1Hz transmission rate. While for this work the advertisement packets did not carry any additional information, the general BLE architecture provides the ability as each packet can be customized to carry up to 31 bytes of data. This payload is able to carry additional sensor measurements for each user (accelerometer, gyroscope, magnetometer readings), enabling our model to go beyond exclusive RSSI-only tracking and become a massively crowd-sensing indoor mechanism and thus left for future work.



(a) Per trial day

(b) Per cell - Weekday Average

Figure 3.4 Edge to Cloud message load

Finally, following the location-aware infrastructure installation, we provided BLE ibeacons to 46 frequent facility occupants to carry during their everyday routine. The trial was approved by IRB (Institutional Review Board for the Protection of Human Subjects in Research) and lasted for approximately one month from September 15, 2016, to October 18, 2016. Fig. 3.4a shows a heatmap that visualizes the overall edge to cloud message load for each day of the experiment. A thorough description of both the testbed setup and the real-subject trial can be found in [144].

3.4.2 Deployment Considerations

At this point, we want to emphasize on two design choices regarding the location-aware infrastructure. First, we favored the use of a BLE-inspired solution over a WiFi-based system. The main reasons for this include the inexpensive nature of BLE equipment that makes the maintenance and installation cost negligible. Also, the minimal power footprint of BLE beacons results to mini-scale devices with long battery life. Moreover, since WiFi was designed exclusively for data transmission, it does not allow parametric changes, with the adjustable transmission rate of BLE beacons being a case in point.

Second, even with the BLE-based architecture, our model follows a moving-beacon fixed-scanner approach which constitutes a departure from the traditional static BLE beacon deployment. Since its introduction, the BLE protocol has been widely popular

among wearables and IoT applications mainly due to its extremely minimal power demands. Therefore, indoor localization applications were among the first to explore the capabilities of BLE in this domain with approaches that span from fingerprint-based systems [91] to infrastructure implementations for museums [12] or marketing and advertisement [76]. However, the majority of these studies deploy static BLE beacons and utilize smartphones or other devices as scanning probes and processing units [337].

We view this method as a burden for phones in terms of power and resource consumption. Moreover, this moving-scanner fixed-beacon approach relies heavily on the assumption that all occupants carry smartphones and they have the specific application and appropriate incentives to use it. Therefore, with our reversed architecture we managed to deploy a large scale prototype relying on low-cost static scanners and a cloud setting by forming a sensing layer of moving transmitters. Finally, and more importantly, we surpassed the challenging and often prohibitive part of finding incentives for a countable amount of users to take part in a long-lasting trial. For these reasons, this approach is gaining popularity lately and is deployed in works like [44], where data were collected from a large number of participants ($\sim$ 900) in a two-day setting staged at a nightclub, or like [162] where an elderly activity monitor was implemented in a restricted 6-room setting.

3.4.3 Data Set and Unsupervised Training

The aforementioned design choices empowered the realization of a real-world setting and enabled the collection of every-day crowd-generated BLE fingerprints (User ID, Edge Device ID, RSSI, Timestamp). The dataset collected during the one-month trial contains over 19M BLE fingerprints from 46 participants following their usual routines [269]. Fig. 3.4b shows the average number of edge to cloud messages that were generated in each facility cell. For cells covered with more than one edge device (see Fig. 3.3) their load was averaged and the scanners were clustered as explained later in this section. Therefore, Fig. 3.4b also reveals area popularity in terms of collected advertisement packets that are transformed into MQTT messages.

This experimental procedure made it possible for us to practically test our crowdsourced unsupervised location-aware facility model. In order to extract our training set, the fingerprints of each user were considered separately and underwent a preprocessing proce-

dure. Following that, we sampled the observed fingerprints using a configurable decision window, that indicates how frequently the central system classifies a user to a cell. During this window the user's advertisements were observed by one or multiple edge devices and therefore, at the end of this decision interval, we average these RSSI observations to produce one single RSSI value, linked to each scanner.

The length of this estimation window can vary depending on the specific scenario we consider for the facility. Our design with the 1Hz beacon transmission rate enables decision periods starting at 1 s destined for micro-location services [335]. However, small decision windows lead to a small number of sampled RSSI values and therefore enforce the known issue of signal strength fluctuation. For this reason, we consider 5 s as the floor of the decision window. Also, since our system aims to facilitate occupant mobility tracking, we consider 25 s to be the duration of our largest estimation window.

At the edge computing layer, thirty Raspberry Pi scanners were totally installed defining two scenarios of sparse (15 devices) and dense (30 devices) deployments. For the localization purposes, we considered twenty-five scanners, as shown in Fig. 3.3, that partition the smart space into 15 cells of 18m grid square side size. In order to retain the basic architecture of our model, we virtually clustered all edge devices that belong to the same cell. To retain fairness, after averaging the RSSI observations of each in-cell scanner we kept the highest to represent the whole cell. This clustering leads to a setting of $N = 15$ cells and edge devices, and therefore to a training feature vector of 15 dimensions. However, when a user is in a given location, his transmissions are observed only by a subset of edge devices. For the rest of the scanners, we assign to its feature variable the value of -115 dBm which is the lowest RSSI value observed during the trial (noise floor).

By performing this type of preprocessing to the dataset we generated for each day of the trial multiple unlabeled sample sets depending on the chosen decision (sampling) window. In essence, the trial participants act as numerous RSSI probes, sampling the space with their movement. In the following section, we examine how these generated daily samples can be used to continuously train the model and produce decent localization results even after the first day of measurements.

Finally, in accordance with the discussion in Section 3.3, we initialize the model parameters $\boldsymbol{\theta} = (\boldsymbol{\pi}, \boldsymbol{\mu}, \boldsymbol{\sigma^2})$ as follows. Using measurements of RSSI vs distance pairs from a single

experiment, we calculated tha basic log-distance signal propagation model [254]:

$$P_d = P_{d_0} - 10\,\alpha \log(\frac{d}{d_0}) \tag{3.7}$$

where P_d and P_{d_0} represent the RSSI (dBm) observed d meters away from the source and the RSSI (dBm) observed at a reference distance d_0 ($P_{d_0} = -64.63$ for $d_0 = 1m$ in our case), respectively. Further, α denotes the path loss exponent that describes the wireless channel and was found equal to 0.8891 with 95% confidence interval. Using this model, we initialize the mean parameter $\boldsymbol{\mu}$ as $\mu_{jc} = P_{d_{jc}}$ where d_{jc} denotes the distance between a user located at the center of cell c and the edge device j that covers a different cell ($j, c \in \{1, ..., N\}$). For the $j = c$ cases, we impute to the initial matrix the value -60 dBm (highest observed RSSI value), while to reduce interaction between floors we set μ_{jc} = -115 dBm (noise floor) when j and c are located in different floors. Finally, the variance parameter $\boldsymbol{\sigma^2}$ is initialized to 5.45 for all components. This value is the experimental mean of the variances that were calculated for each test distance during the channel modeling measurements.

3.5 Performance Evaluation

This section presents the evaluation of the proposed location-aware facility solution and discusses a number of variations. The test cases include different model training approaches, examining variables such as the size of a training set, the size of the decision window, and a number of utilized model features. Moreover, we evaluate the ability of the model to track user mobility and the impact of different installation scenarios in facilities with a fluctuating number of visitors.

To thoroughly evaluate our design, we collected a large number of labeled samples $\boldsymbol{s}^i_{test}$ from each cell following the procedure described in Section 3.3. These labeled samples are used for validation and testing purposes and were extracted from a variety of spots inside each cell including both near center and cell limit locations. All measurements were taken by a single test user whose exact location and cell was known and continuously monitored. After initialization and training, the model was used to compute the cell estimate for each test sample $\boldsymbol{s}^i_{test}$ and classify it to a cell c. Given the actual and estimated labels,

we utilize the metrics of accuracy, error rate, precision and recall/sensitivity. These metrics are widely used in evaluating machine learning settings, for example, [282]. To this end, since we examine a multi-class classification model with $N = 15$ classes/cells, we used a 15 class confusion matrix that assumes One-vs-All (OvA) classification and defines for each cell/class i the parameters:

- True Positives (TP_i) - Number of cell i test samples classified to cell i
- True Negatives (TN_i) - Number of test samples not extracted from cell i and not assigned to cell i
- False Positives (FP_i) - Number of test samples not extracted from cell i and incorrectly classified to cell i
- False Negatives (FN_i) - Number of cell i test samples not classified to cell i

Given these definitions, we form our metrics as follows:

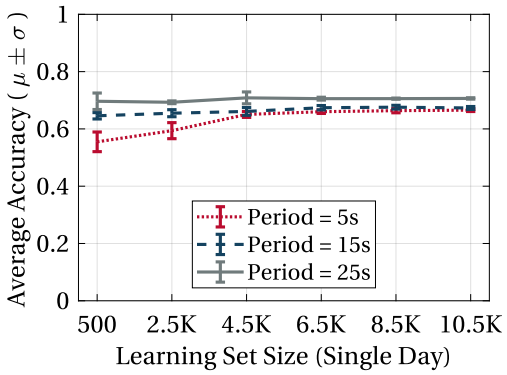
$$\texttt{Overall Accuracy} = \frac{\sum_{i=1}^{N} \frac{TP_i+TN_i}{TP_i+TN_i+FP_i+FN_i}}{N}, \tag{3.8}$$

$$\texttt{Precision} = \frac{\sum_{i=1}^{N} TP_i}{\sum_{i=1}^{N} TP_i + FP_i}, \tag{3.9}$$

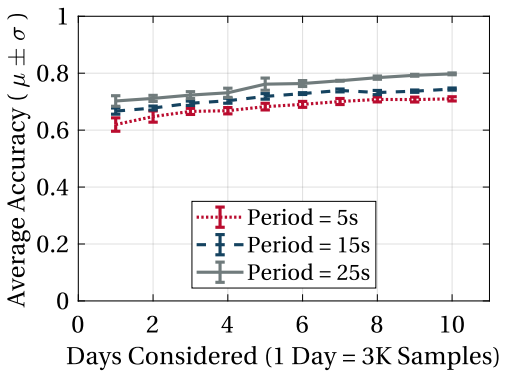
$$\texttt{Sensitivity/Recall} = \frac{\sum_{i=1}^{N} TP_i}{\sum_{i=1}^{N} TP_i + FN_i}, \tag{3.10}$$

where `Accuracy` represent the fraction of correctly classified samples, and `Precision` the overall ratio of correct positive predictions. `Recall` represents the overall ratio of correctly predicted positive observations to all observations of the class and `Error Rate` = 1 - `Accuracy`.

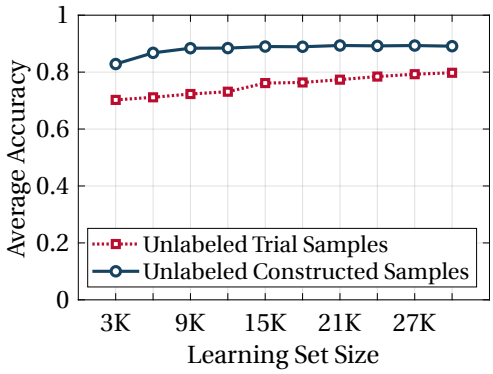
Finally, a remark should be made regarding our choice to evaluate our design with a single user. During early testing with multiple test users simultaneously located in different areas, individual average accuracy results revealed negligible differences. Therefore, for simplicity, a single test user was finally used to conduct the extensive testing on various locations and along with different path variations. We can safely report that for the case



(a) Single day samples



(b) Multi-day samples



(c) Constructed samples

Figure 3.5 Unsupervised Learning: Average accuracy vs. learning set size

of a lightly crowded same-scale facility (1-20 users) the proposed system's accuracy will coincide with the following results.

3.5.1 Unsupervised Approach

The main feature of our model is the use of unlabeled samples extracted by the every-day interaction of the visitors with the smart space. In that sense, we used our trial dataset to train our GMM model. The fingerprints from the dataset were sampled for each user with time intervals of 5, 15, and 25 seconds. The same happened for the fingerprints taken during the testing phase. These periods correspond to the central decision window, mentioned

in Section 3.3. Depending on this window we had training sets of different sizes. To retain fairness we used for each model training procedure the same number of samples regardless of the sampling window.

Fig. 3.5a shows the average accuracy and standard deviation of the user cell classification when the training samples belong to a single day of the trial. Each time a total of 10 models were trained with different training samples randomly permuted. Following that, we examine the classification accuracy when more days are considered for the learning process. For each new day, regardless of the decision window, additional 3000 training samples were randomly chosen to train the model. Therefore, at the same time, we examine the accuracy as a function of the learning set size, since on the tenth day we will finally evaluate 30K training samples. The results are shown in Fig. 3.5b. For each new day/sample addition, the model was retrained with the aforementioned initialization parameters.

Regarding the decision window, evidently larger sampling intervals lead to better classification results. This is explained due to the fact that during longer windows the system collects and averages more RSSI values to generate each training and testing sample. Therefore, the model is trained with samples of higher quality, even when the user is moving at that moment.

Another interesting observation emerging from the unsupervised training analysis is the rise of classification accuracy when more days are considered in the learning process. On the contrary, simply increasing the 1-day generated training set size leaves performance almost in steady-state after one point (i.e., 4.5K, see in Fig. 3.5a). This can be explained by the unsupervised nature of the setup that does not lead to uniform spatial sampling. When a limited number of days is considered there might be areas inside the facility not visited as often as others or even not visited at all. This reflects the area/cell popularity and results in training sets with denser data for some cells as opposed to others (misrepresented cells). This phenomenon can also be seen in Fig. 3.4b, where an absolute number of messages per cell indirectly reveal their popularity during the trial. Therefore, as observed in Fig. 3.5b by keeping a low amount of training samples for each day (3K) and increasing the number of days considered we manage to train our model with a more diverse set of samples resulting in the overall accuracy of up to 81% after ten days of trial and for 25 s estimation window.

In order to examine the impact of uniform space sampling in our model performance, we constructed a set of samples uniformly distributed among cells. The samples were

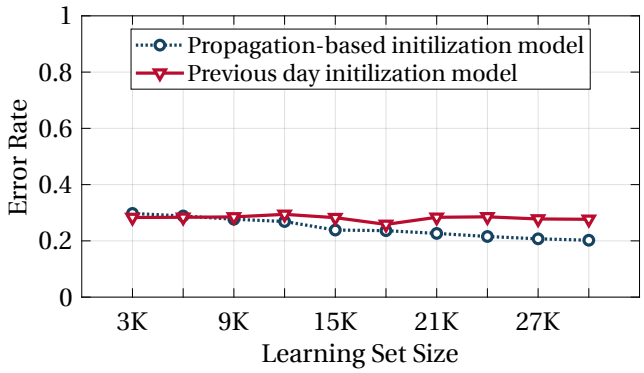


Figure 3.6 Unsupervised: Error rate vs. learning set size for different initialization models

constructed using a GMM with characteristics extracted from the real measurements given the 25 s RSSI sampling. Using this set, we trained and evaluated models by gradually increasing the number of uniform samples to corresponding with the per day trial samples. Fig. 3.5c shows these results.

3.5.2 Initialization Variations

As explained above, the use case for our setup assumes that the infrastructure (and its operator) collects each day more and more training data without any labor cost and the GMM localization model is rebuilt and updated incrementally. In this procedure for each new model training, although we use more training samples, we utilize the same initialization propagation-based model we developed once as described in Section 3.4. Since the EM algorithm converges to a local optimum, the initialization process plays an important role in the performance. Therefore, we now test a different approach to our incremental training process. For each new day's model training, we use as initiating model the one constructed during the previous day. Fig. 3.6 shows the comparison of these two approaches. The use of the previous day's model initially yields similar results but as the learning set size increases the new approach fails to increase accuracy.

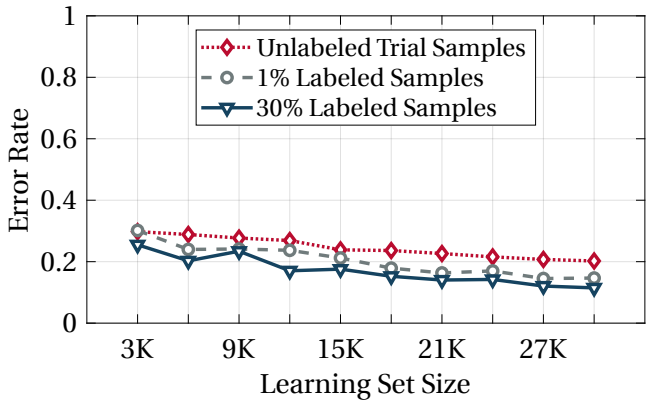


Figure 3.7 Semi-Supervised: Error rate vs. learning set size

3.5.3 Semi-Supervised Approach

Given the described infrastructure setting, gathering unlabeled data from the users is a virtually labor-free task. In all fingerprinting-based systems, the main setup cost arises from the labor-intensive task of gathering labeled fingerprints mainly through war-walking procedures. In this Section, we explore how semi-supervised training using both labeled and unlabeled samples affects the classifier's performance.

To that end, we used a part of our test samples as labeled learning samples to train our model in the semi-supervised sense we discussed in subsection 3.3. Again, we utilized unlabeled samples extracted by the users and from each day, while as a decision/sampling window we picked the 25 s setting. For fairness, we will keep the number of total samples from each day steady (3K), while regarding the labeled portion we examine two cases utilizing 1% of labeled samples (≈ 30/day) and 30% of labeled samples (≈ 900/day). Fig. 3.7 shows the intensity of performance increase along with how such a system would learn over time (here in the course of ten days). The error gradually improves with time and more data samples. This improvement will continue until a certain saturation point.Finally, Table 3.1 summarizes the performance of the model for various settings when for the learning process samples from 10 trial days were utilized.

Table 3.1 Performance evaluation for various learning settings

Setting	Accuracy	Precision	Recall
5 sec Window	0.711	0.640	0.652
15 sec Window	0.744	0.799	0.662
25 sec Window	0.798	0.847	0.735
25 sec Window - Constructed Samples	0.891	0.901	0.894
25 sec Window - 1% Labeled	0.853	0.871	0.766
25 sec Window - 30% Labeled	0.885	0.878	0.819

3.5.4 Tracking Mobility

Until now, all testing samples were gathered from a stationary test beacon/user. However, an important feature of a location-aware facility is the ability to track the occupants' mobility at all times. By design, our infrastructure model provides full simultaneous supervision of edge devices to the central cloud-based decision system. Therefore, it can monitor the cell transitions of all users in real-time as depicted in Fig. 3.8a. To do so the model after training uses real-time RSSI vectors/samples to classify a visitor to a cell for each decision window time interval. An important factor regarding this technique is the size of the decision window and how it affects the accuracy of trajectory estimation. To evaluate this mobility tracking ability, we performed a set of focused experiments where a user followed, at a walking pace, a predefined point A to B path crossing several cells in the process. Starting and finishing points were located at the center of the cells, while path lengths varied from 18 to 108 meters. To measure performance, we express actual and estimated routes as path strings where each new character indicates a cell transition, as denoted in the description of Fig. 3.8a. Following that, to extract the deviation between the actual and estimated paths, we utilize a custom error metric and compute the Normalized Levenshtein Distance [333] also known as Normalized Minimum Edit Distance between two strings [191]. Zero Normalized Levenshtein Distance value signifies total overlap between real and estimated paths.

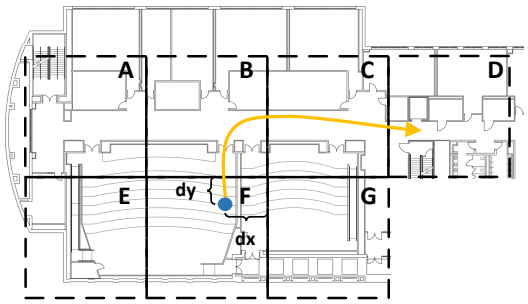
For each path test, we sampled the raw fingerprints with different decision periods, and

created separate sequential path test samples to be given as input to our trained model. For fairness, we used the same unsupervised 15-feature model during the process, trained with the 25 s window set of 10-day samples (see Table 3.1). Fig. 3.8b shows the mean and standard deviation of the path error when different estimation windows are considered, while Fig. 3.8c associates the error with the tested path length. All fitted lines are exponential fitted curves with 95% confidence bounds.

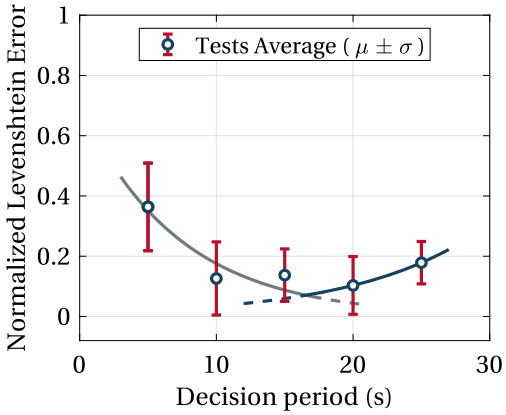
For small decision windows (e.g., 5s), there are mainly two factors contributing to the path error. First, for a given path duration the system performs more cell classifications per time interval. Second, small decision windows equal to poor RSSI sampling, which is a parameter that can have a huge impact regarding the accuracy of systems that rely merely on signal strength measurements [337]. Interestingly, the shift towards extended decision intervals (e.g. 25 s) also fails to trace the real path with high confidence. In some cases, the user's walking frequency exceeds the decision period leading to the omission of cells and lower path tracking performance. Therefore, depending on the facility type the decision period is a variable that should be carefully calibrated. Alternatively, higher beacon transmission rates (>1 s was used in our trial) can provide larger sets of RSSI measurements to be averaged, which is a process that can also be moved to the edge, with the scanners performing the sampling.

3.5.5 Comparative Analysis

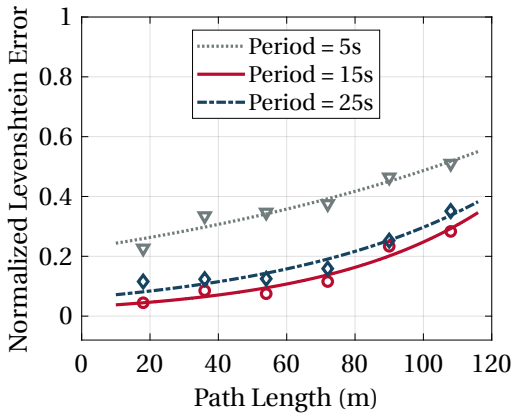
In this Section, we perform a comparison regarding the system's performance considering static and mobile users along with a different localization mechanism. Initially, we compare our unsupervised learning approach with a deterministic cell classification method. According to the latter, given the RSSI measurements observed in several edge devices, and originated by a given occupant, he is assigned to the cell/edge device where the highest RSS value was collected. Thus, we perform a deterministic assignment with the absolute value of the RSSI measurement as a criterion. For the unsupervised learning approach, we used the same unsupervised 15-feature model, trained with the 25 s window set of 10-day samples (see Table 3.1). Fig. 3.9a shows the average error rate of cell assignments when a user is static in a certain cell (averaged from several locations in the three-floor setting) vs. the system's decision period. Fig. 3.9b focuses on moving users and depicts average



(a) User cell transition: $F \rightarrow B \rightarrow C \rightarrow D \equiv$ "FBCD"



(b) Error vs. Decision Period

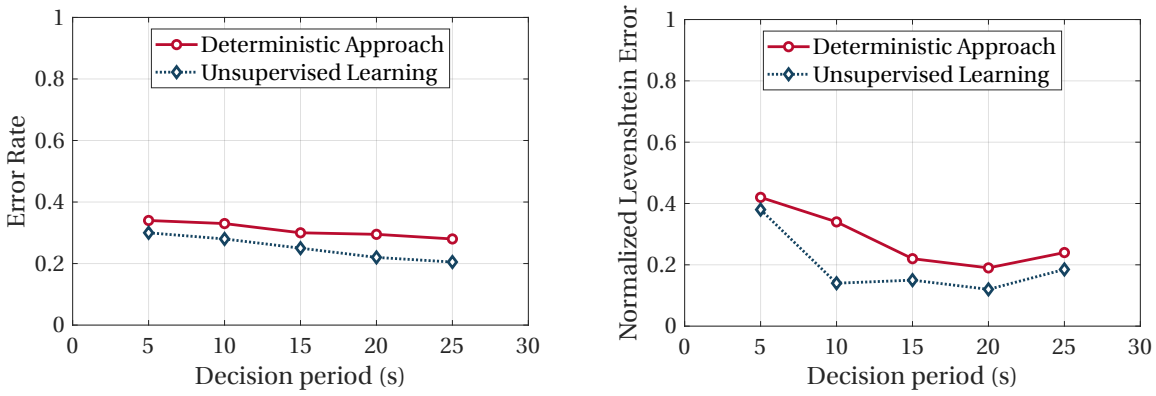


(c) Error vs. Path Length

Figure 3.8 Mobility tracking and performance

normalized Levenshtein distance error (see Section 3.5) of multiple point A to point B path tests in same-floor, and inter-floor cases, against increasing system's decision period. The proposed procedure yields superior performance results for both cases with the user locations near cell borders being the main contributors to the error.

Next, we focus on the performance of the proposed unsupervised approach comparing the cases of static and mobile occupants using average error expressed in meters. Since our system by design classifies occupants in discrete cells and given the known exact location of the test user, the distance error is computed as follows: for a cell misclassification case,



(a) Static user

(b) Mobile user

Figure 3.9 Deterministic cell classification vs. Unsupervised learning-based cell classification

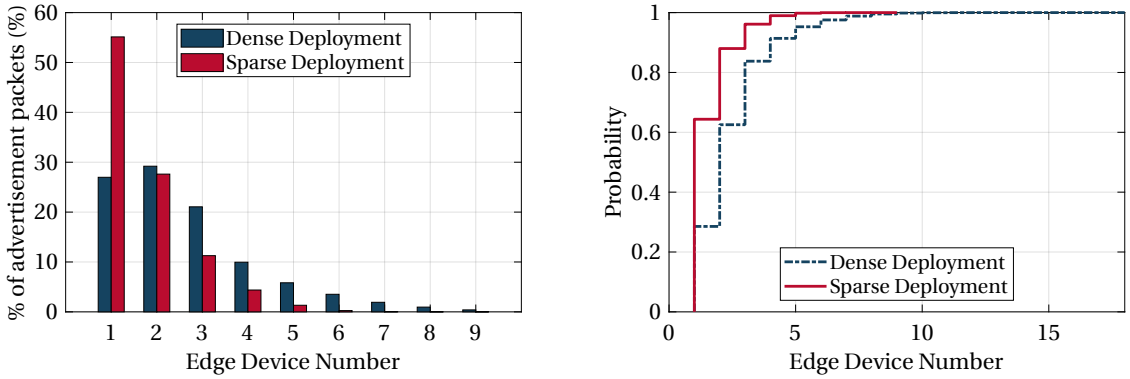
the distance error equals the Euclidean distance between the test user's position (inside the correct cell) and the border of the wrong cell output. Considering Fig. 3.8a for a visual example, the distance error of the user misclassification to cell G equals to dx, the error from a misclassification to cell B equals to dy, while for cell C the distance error equals to $\sqrt{(dx)^2+(dy)^2}$. Table 3.2 presents these results comparing the cases of static users vs. users following predefined point A to point B paths. Different classification decision periods are considered implementing the unsupervised 15-feature model, trained with the 25 s window set of 10-day samples. Note that for the case of mobile test users their path was discretized using 1-meter intervals. For the static user cases average errors remain low for large decision periods due to the increased RSSI averaging window. On the contrary, the mobile users' average location accuracy varies depending on their moving pace, along with the overall decision period since an increased decision window fails to capture fast pacing users.

3.6 Deployment Impact

This section discusses how the installation of our IoT-based system in a real-world infrastructure can affect design decisions. One of the main characteristics of real-world IoT settings is their ability to generate a massive amount of information which can be a challenge for both the network and the respective back-end which in most cases will be

Table 3.2 Proposed System's Average Distance Error

Desision Period (s)	Average Distance Error (m)	
	Static User	**Mobile User**
5	5.252	6.586
10	5.022	5.072
15	4.608	5.271
20	3.742	4.658
25	3.245	5.015



(a) Percentage of simultaneous receptions **(b)** pdf of random variable E

Figure 3.10 Multiple edge devices receiving the same advertisement packet - Dense vs. Sparse deployment

cloud-based. In our architecture (see Fig. 3.1), the same advertisement packet generated by a single beacon/user can be received by multiple edge devices. This inevitably leads to the creation of possibly multiple edge-to-cloud messages for every user advertisement (not 1 to 1 correlation).

We define two deployment scenarios to explore this phenomenon in association with the edge device density in the given facility area, a dense (30 active scanners) and sparse scenario (15 active scanners). Following that, we utilize the 30-day trial measurements (user fingerprints) to calculate how the unique BLE advertisements were distributed with respect to the number of different scanners that intercepted them. Fig. 3.10a depicts those

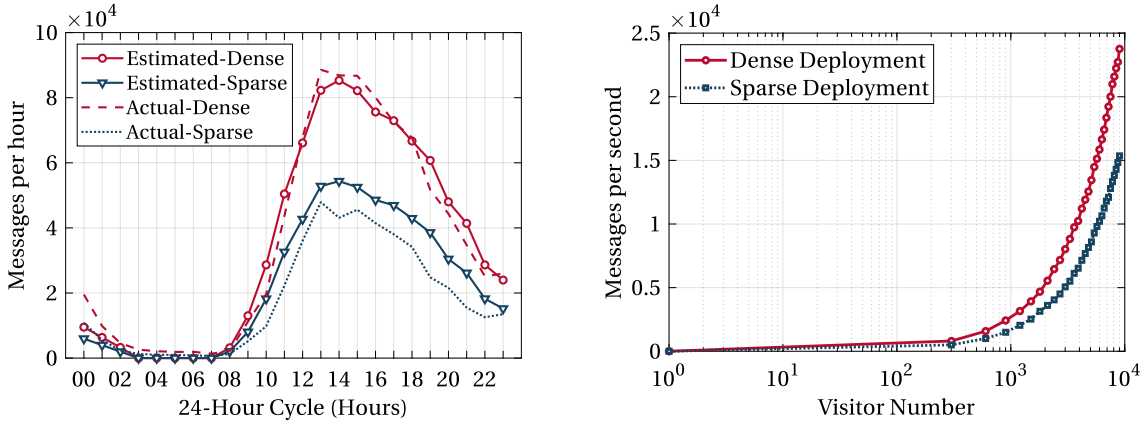


Figure 3.11 a) Estimated and actual no. of trial messages/hour (weekdays average), b) Messages/sec as a function of visitors.

results, where in the case of a sparse deployment scenario, 55% of the transmitted unique packets were received by strictly one edge device and 28% by strictly two scanners, etc. For the dense deployment, these values change to 27% and 29%, respectively.

Relying on those experimental measurements, we define a discrete random variable E that represents the number of edge devices that intercept an occupant's single beacon transmission. We construct two variations of this value. The first is associated with a sparse installation of scanners with pmf $p(E = e|Sparse)$ with $e = e_S \in \{1,...,9\}$, while the second with a dense installation with pmf $p(E = e|Dense)$ with $e = e_D \in \{1,...,18\}$. The cdf of these random variables is shown in Fig. 3.10b. Given the number of active occupants k inside the facility, and the exact transmission rate of their beacons (1Hz in our case), we can generate an estimation of the produced traffic (MQTT messages) towards the cloud as $messages/sec = \sum_{i=0}^{k} E$.

We evaluated the aforementioned formula using the average number of trial participants seen inside the facility throughout a day. Using their variable number k, we estimated the expected number of messages per hour and compared them with the actual values as shown in Fig. 3.11-a. While the impact of message creation volume may be negligible in settings like our testbed (small facility & number of active visitors), this might not be the case for larger facilities like stadiums or museums, where the functionality of our systems takes the form of crowd monitoring. In such cases, message generation will affect the available throughput of the network, and further quantities related to the cloud resources (e.g., queuing services,

computing, memory, and storage) that should be provisioned. Therefore, estimating the expected message load is crucial to support proper capacity planning for the location-aware infrastructure. Fig. 3.11-b presents a projection of generated traffic when the number of active occupants is increasing.

At this point, we should note that we examine traffic generated between the layers of edge computing and centralized cloud (see Fig. 3.1). Regarding the beacon-based communications between the sensing and edge layers, large user numbers can result in a certain blocking rate depending on the chosen technology. An overview of this phenomenon for the BLE case can be found in [166] and [133]. Possible solutions for this issue include the installation of multiple edge devices per cell or the definition of micro cells inside bigger ones in frequently overcrowded facility areas.

3.7 Discussion

Most of the aforementioned studies show competitive localization accuracy results, given the specific utilized hardware and their experimental setting. However, given the nature of the approaches that rely on RF fingerprinting, in accordance with the unpredictability and fluctuation of RSSI readings in indoor spaces, they exhibit high dependencies on possible landscape changes, varying visitor densities, and occupant mobility. Therefore, the proposed approach that depends on the specific crowd densities or user group numbers anticipated to occupy the facility aims to mitigate such dependencies by gathering samples during various occasions and by repeating the training process. This advantage that essentially treats the sensing environment as a black-box can also reduce localization errors when the facility environment and landscape changes, which is considered common for indoor settings. In addition, the unsupervised nature of the training procedure along with the proposed moving-beacon fixed-scanner architecture results in a substantial simplification of the manual site survey that is the main effort cause in supervised and semi-supervised settings.

Moreover, our implementation creates a president for IoT-equipped BLE-enabled facilities where localization services are practically embedded inside the infrastructure. Consequently, this setting can also physically act as an indoor crowdsensing platform either

in the participatory sense (i.e., active involvement of the user to collect information) or in the opportunistic sense (i.e., minimal user participation in the data collection). This functionality is highly desirable in several facility types ranging from museums (exhibit popularity monitoring, visitor Quality of Experience (QoE) enhancement), to stadiums (crowd motoring and managing applications). Also, such architecture enables IoT-based public safety applications that can be aided by wireless beaconing (users broadcasting their locations), or future establishment of Device-to-Device (D2D) communications between occupants (sharing location information, or acting as mobile gateways).

Also, apart from a Bluetooth-based big-scale implementation president, the proposed learning-based approach can essentially lead to better localization results as new observations are introduced in the training process. This claim is supported by our initial results where for the 25s decision period case the unsupervised model showed a 10% accuracy increase as the considered trial days were increased from 1 to 10. Also, since the trial considered occupant traffic generated under real conditions, this work presents a real-world IoT-based user localization scheme that provides insights on the message load that should be anticipated in similar cases.

Finally, there might be system accuracy changes related to the crowd density variations at a given time. In a heavily crowded area (e.g., 100-500 users) one might expect RF signal propagation variations. However, in our case given the size of the corridors and rooms, we do not believe this is an issue. We consider the case of intensively crowded facilities (e.g., stadiums, malls) as future work that will shed light on performance variations of multi-tenant simultaneous presence since then the RSSI fluctuations will be considerable.

3.8 Related Work

Indoor localization relying merely on RSSI-measurements is a well-explored topic, especially through the prism of RSSI fingerprint matching. Such solutions require an extensive measurement collection to feed a calibration phase that builds a radio-map, which is essentially a database of indoor locations associated with wireless fingerprints. Such radio-maps can have various forms and usually follow either deterministic (i.e., specific RSSI values are associated with discrete locations) or probabilistic (i.e., location-RSSI relations are

represented with statistical values) models depending on the designed system [150]. Following the radio-map construction, an active localization phase is realized to classify online wireless fingerprints to indoor locations.

Although the fingerprinting localization approach presents a significant number of physical limitations [322] and challenges related to utilized device diversity [316], it has steadily been the forefront of indoor localization systems. Among the related literature, researchers utilize different machine learning techniques to construct the radio-map models and consequently realize the localization processes. In this section, we review the different techniques that rely merely on RSSI readings. We focus on the learning approach variations and the effort that each work requires in terms of fingerprint collection. We will not review solutions such as Zee [235], WILL [326] or LiFS [325] that combine fingerprint matching with readings from Inertial Measurement Units (IMUs) and dead reckoning techniques since they constitute a different problem setting.

The pioneering and extremely popular fingerprint-based system RADAR [25] relies on k-Nearest Neighbour (kNN) averaging to estimate desired locations and use a deterministic radio-map model. In contrast, a probabilistic model is used in the WiGEM WiFi-based system [118] where a Gaussian Mixture Model is trained using labeled samples and the EM algorithm. Lately, enhanced machine learning methods have been deployed to take advantage of the fingerprinting data. The DeepFi system as reported in [320] exploits channel state information (CSI) instead of the usual RSSI readings to train offline a localization model using deep learning and a greedy learning algorithm.

All aforementioned methods utilize supervised learning with training samples accompanied by a known location. Therefore these approaches highly depend on the quality of the samples that are usually gathered after extensive labor-intensive site-surveys. Also, since wireless channels in indoor environments are highly unpredictable due to shadowing effects, the offline fingerprint collection process should be repeated in case of a major landscape change or changes concerning the wireless access points used.

In an attempt to reduce such labor-intensive site-surveys researchers started considering the use of unlabeled fingerprints as complements to the labeled measurements. This has lead to a research stream that utilizes semi-supervised learning techniques to extract radio-map models. In this category, the EZ system [61] requires no prior configuration and utilizes a genetic algorithm that relies on gradient descent to make the fingerprint to loca-

Table 3.3 State-of-the-art learning-based fingerprinting indoor localization solutions.

Work	Learning Method	Technique	Effort	Average Accuracy
RADAR [25]	Supervised	k-NN Averaging	Labeled Fingerprints (100%), Floorplans	2-3 m
WiGEM [118]	Supervised	GMM - Expectation Maximization	Labeled Fingerprints (100%), Floorplans	4-6 m
DeepFi [320]	Supervised	Deep Learning Channel State Information Features	Labeled Fingerprints (100%), Floorplans	0.94-1.8 m
EZ [61]	Semi-Supervised	Genetic Algorithm	Unlabeled Fingerprints Labeled Fingerprints (6-15%)	2 m, 7 m
Chai et al. [52]	Semi-Supervised	HMM - Expectation Maximization	Unlabeled Fingerprints, Floorplans Labeled Fingerprints (< 50%)	60-90% (< 3 m)
Sorour et al. [284]	Semi-Supervised	Manifold Learning	Unlabeled Fingerprints, Floorplans Labeled Fingerprints (< 50%)	2-4 m
LARM [217]	Semi-Supervised	Manifold Learning Graph Laplacian, Dead Reckoning	Unlabeled Fingerprints, Floorplans Labeled Fingerprints (< 25%)	< 40% (relative error)
Mohammadi et al. [197]	Semi-Supervised	Deep Reinforcement Learning	Unlabeled Fingerprints, Floorplans Labeled Fingerprints (∼ 16%)	∼6 m
Jung et al. [151]	Unsupervised	k-means, Memetic Algorithm	Unlabeled Fingerprints, Floorplans	2.7-3.1 m
Li et al. [181]	Unsupervised	Bayesian HMM, Particle Filtering	Unlabeled Fingerprints, Floorplans	80% within 1.5 m

tion connections. In [52] unlabeled fingerprints are coupled with labeled measurements to train a Hidden Markov Model (HMM) using an EM-based algorithm. Another popular technique adopted in the semi-supervised approaches is manifold learning. In [284], the authors describe a localization system that requires limited offline calibration and utilizes manifold alignment to discover correlations between unlabeled fingerprints and locations in a low-dimensional learning space. Similarly, in [217] the LARM system utilizes a graph-based manifold learning strategy to infer a final localization model with reduced need for labeled samples. Finally, in [197] authors developed a BLE-based localization system deviating from the usual WiFi-based approaches. Their solution deploys a semi-supervised approach that exploits deep reinforcement learning and the statistical information of the unlabeled measurements.

These methods still require a countable amount of location labels to accompany the RSSI samples. There exist a few studies that solemnly rely on crowdsourced RSSI measurements and extract radio-map models only from unlabeled samples. Such crowd-assisted solutions move the load of site-surveys to the multiple users/indoor space occupants. For example, an HMM-based method was utilized in [151] to model unlabeled user traces towards building a crowdsensed localization system. More specifically, the solution combines a population-

based evolutionary algorithm with unsupervised calibration and utilizes segmental K-means to perform local parameter optimization of the initial models. Finally, a hierarchical Bayesian HMM model coupled with particle filtering was utilized in [181] for hidden state estimation that results in a system where a site survey is no longer required.

Table 3.3 summarizes the related works as discussed in this section. They are classified according to the learning approach used and the effort required for each in terms of the required data type. Unlabeled fingerprints are considered relatively easy to collect, and usually, crowdsourcing techniques are applied to eliminate any extra interventions. Labeled measurements are more costly in terms of manual-labor and site-surveys involving war-walking. The average accuracy is reported as found in the related literature. It should be noted that these values do not provide a fair comparison as the results highly depend on the respective experimental environment and the specific wireless protocol and equipment used.

3.9 Conclusion

In this chapter, we propose a three-tier sensing infrastructure that combines data beaconing, and an IoT-inspired edge computing setting coupled with a centralized cloud decision level. This next-generation facility deployment supports the collection of user-centric data along with user localization services implemented by a probabilistic cell-based GMM. A key innovation is the use of crowdsourced fingerprints to employ unsupervised learning of the localization model. This approach eliminates the need for exhaustive site surveys to construct and renew the facility radio maps. As part of the evaluation process, we have deployed an experimental multi-story facility testbed and collected data via a real-world large-scale trial. Results reveal average location classification accuracy of 0.8 for the unsupervised setting while it can go up to 0.9 when a semi-supervised strategy is considered. Our analysis highlights how parameter and deployment variations can impact localization accuracy and general deployment planning. Finally, the extensive trial dataset can be utilized to extract a single user's movements over time and therefore reveal mobility patterns that can further enhance the localization accuracy.

Chapter 4

Heterogeneous Public Safety Networks

An edited version of this chapter was originally published in [273].

4.1 Introduction

Public Safety Networks (PSNs) are responsible for establishing resilient and reliable communication during public safety (PS) threatening events and can lead to a successful response and post-disaster management in smart cities. Their operation in disaster-struck areas is paramount as they (a) aid the communication coordination (critical information exchange) among emergency management agencies (first responders, law enforcement, medical personnel, rescue squads), (b) provide general public situation awareness and lead to smooth adaptation of emergency management protocols (alerts, evacuation policies), and (c) ensure the information exchange (e.g. video, voice, data) in cases of degraded or failing critical infrastructure (e.g. base stations) [26, 168]. Moreover, PSNs are usually established in challenging environments with multiple involved agencies, conditions of panic for the civilian population, and degraded communication infrastructure. Thus, their design and architecture should account for several attributes, including fast deployment, adaptive operation, coverage guarantees, low latency, and most importantly extended energy availability for the PSN nodes.

Traditional PSN architectures have been relying on dedicated cellular networks such as the narrowband time-division multiple access (TDMA)-based TETRA (Terrestrial Trunked

Radio) [83] or Project 25 [189] that require specialized hardware and offer low data rates [168]. More recent designs rely on the broadband LTE technology [80, 227] that offers among others large-scale deployment and support of multiservice scenarios (multicast or broadcast service support). Recent additions to the public safety LTE offerings list include proximity services and Device-to-Device (D2D) communications, as introduced by the Third Generation Partnership Project (3GPP) Releases 12 and 13 [1].

Thus, the related research now focuses on approaches that increasingly utilize commercial public user equipment (UE) and on single wireless network protocol (WNP) architectures that include D2D communication capabilities. These attributes can increase PSN's energy autonomy and capacity, reduce latency, and account for critical infrastructure failures that can threaten the information flow. However, the PSN models proposed until now ignore: (a) the ability of modern UEs to utilize, apart from the cellular option, multiple wireless communication protocols (e.g., WiFi tethering, Bluetooth, NFC, etc.), which is of paramount importance in PSNs, where part of the cellular infrastructure can be damaged, thus the users should dynamically choose an alternative WNP for communication, and (b) the integration of heterogeneous Internet of Things (IoT) architectures into city and facility infrastructures with the form of multi-sensing multi-protocol devices [232]. This utilization of multiple WNPs in establishing the PSN can exploit the specific characteristics of each protocol and provide UE battery-life extension, sophisticated resource management, interference mitigation or congestion avoidance, and even ensure communications in cases of cellular coverage absence (e.g., critical infrastructure failures).

Regarding wireless network protocol (WNP) selection, most approaches [59, 190, 339] (see subsection 4.7) have considered the problem in a static manner, without the users being able to sense their communication environment and dynamically adjust their choices. Despite the advances that have been achieved in these works, the lack of dynamicity and flexibility in their operation limits their potential exploitation and adoption in a realistic scenario. For instance, during a catastrophic event, where part of the cellular infrastructure fails, motivated by the humans' urgent need for communication we should exploit in a dynamic manner different WNPs and coalition formation alternatives to establish an energy-efficient communication.

In this chapter, we address exactly this issue by introducing the notion of a flexible and dynamic heterogeneous (multi-protocol) PSN, with UEs that support both D2D and cellular

communications. The main contributions of this research work are summarized as follows:

- Software-defined WNP selection by the PSN UEs, who simultaneously consider the system-specific parameters, e.g., PS-environment and topology, protocol specifications, and PSN energy availability. This capability is explicitly addressed via an adaptive reinforcement learning (RL) method.
- A context-aware coalition formation and coalition head (CH) selection mechanism among the PSN UEs that jointly consider UE communication interest and spatial related parameters. Our proposed mechanism utilizes a modified Chinese Restaurant Process (CRP) of low complexity [109].
- A transmission power allocation mechanism is introduced. Each PSN UE is associated with a utility function that represents its Quality of Service (QoS) prerequisites during PS-threatening situations. A maximization problem of each UE's utility is formed and confronted as a non-cooperative game concluding to a unique Nash equilibrium (NE) point.

The rest of this chapter is organized as follows: Section 4.2 describes the system model; Section 4.3 presents the software-defined WNP selection learning-based procedure; Section 4.4 introduces the context-aware coalition formation process; In Section 4.5, the energy-efficient power allocation problem is formulated and solved; Section 4.6 presents a detailed numerical and comparative evaluation. Section 4.7 summarizes related work, and Section 4.8 concludes the chapter.

4.2 System Model

A heterogeneous wireless PSN is considered consisting of $|M|$ UEs whose set is $M = \{1, ..., m, ..., |M|\}$, located at a square critical area and served by a Data Aggregator (DA). The UEs are able to form $|C|$ coalitions among them with $C = \{1, ..., c, ..., |C|\}$ being the set and $|M_c|$ denoting coalition's c size. Each coalition has a coalition-head $ch_c \in M$ which collects the members' uplink transmissions/data and forwards them to the DA. This networking architecture is considered to improve the energy-efficiency of the UEs' communication

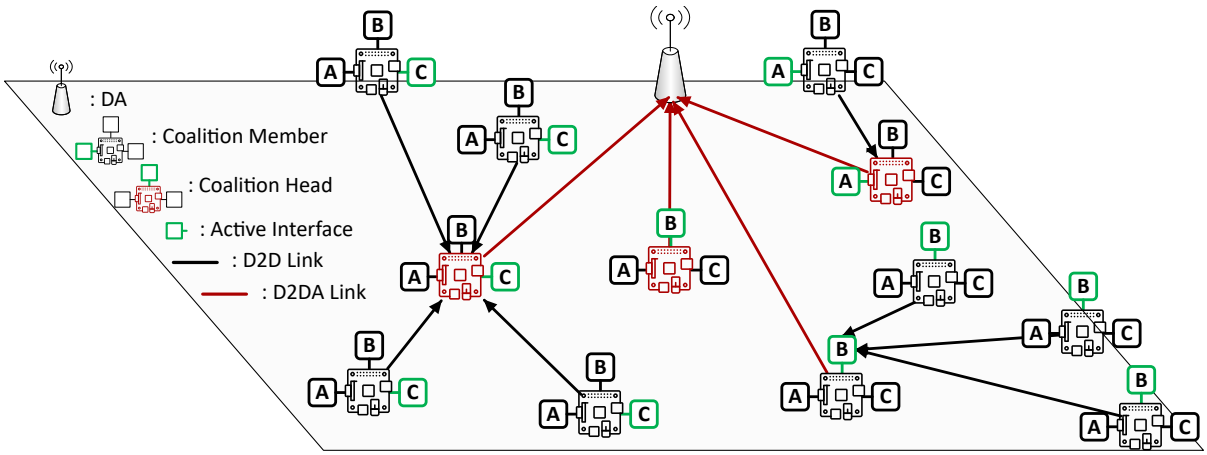


Figure 4.1 Heterogeneous Public Safety Network topology

and decrease the overall PSN's congestion. Specifically, the ch_c collects data from UEs with whom it has high communication interest and are located in a close distance, and reports the data to the DA with fewer transmissions, due to the aggregation potential, and with lower energy consumption. Please note that, if all the UEs were transmitting directly to the DA, they would spend significantly more energy due to their larger distance from the DA, compared to the ch_c, and due to the need for multiple longer transmissions. The UEs are assumed identical in regarding their characteristics, being able to support $|J|$ wireless protocols whose set is $J = \{1, ..., j, ..., |J|\}$, while a uniform distribution of the traffic among UEs is considered. Each UE, by utilizing a single protocol j per timeslot, can communicate either (a) with another UE (D2D) or (b) directly with the DA (Device-to-DA: D2DA). The UEs are considered static per each examined timeslot. For each protocol j,we define specific operational characteristics, namely:

- $d_{range,j}$, which is the WNP transmission range and
- $f_j(\gamma_m)$, which is an efficiency function for each protocol j and expresses the successfully transmitted bits between the transmitter m, and the receiver.

As γ_m we denote the signal-to-interference-plus-noise-ratio (SINR), with each efficiency function f_j being proportional to each protocol's modulation and coding scheme and differentiable, continuous, and increasing with respect to γ_m. We assume that f_j has a sigmoidal-like shape, where γ_m^{target} is its inflection point. Without loss of generality, we

adopt $f_j(\gamma_m) = (1-e^{-A_j\gamma_m})^{M_j}$, with A_j, M_j being real valued positive parameters that control the slope of the sigmoidal functions for each protocol j.

We further assume that regardless of the WNP selection, all UEs operate under NOMA (Non Orthogonal Multiple Access) to cope with the generated interference. The channel gain between a transmitter m and a receiver m' ($c\,h_c$ or DA) is defined as:

$$G_{m,m'} = \frac{K}{d^2_{m,m'}} \tag{4.1}$$

where $K > 0$ represents the channel fading, $d_{m,m'}$ is the distance between UEs m and m'. Under the NOMA Successive Interference Cancellation (SIC) technique [184], the channel gains pertaining to UE m (receiver) are sorted as $G_{|M|,m} \leq ... \leq G_{t,m} \leq ... \leq G_{1,m}$, and the interference sensed by the m^{th} UE is

$$I_m(\mathbf{P_{-m}}) = \sum_{m' \geq m+1}^{|M|} G_{m',m} P_{m'} + I_0 \tag{4.2}$$

with $\mathbf{P_{-m}}$ being the uplink transmission power vector of the rest UEs, and I_0 denoting the thermal noise. The SINR of UE m to a receiver k is

$$\gamma_m(P_m, \mathbf{P_{-m}}) = \frac{G_{m,k} P_m}{I_k} \tag{4.3}$$

where P_m is the UE's transmission power and I_k is the receiver's sensed interference. The aforementioned public safety network topology is illustrated in Fig. 4.1.

4.3 RL-based Wireless Protocol Selection

In this section, the dynamic software-defined WNP selection process is described via exploiting the reinforcement learning. Such an approach enables each UE to perform the WNP selection in an autonomous manner. Specifically, each UE selects to operate under a wireless protocol j by acting as a learning automaton that senses the environment and considers previous action history. Initially, the proposed system constructs a reward probability $r_j(t)$ that collectively reflects the "competitiveness" of each WNP j for the

upcoming timeslot, as follows:

$$r_j(t) = \frac{\sqrt{\frac{ce_j}{\underset{\forall j \in J}{sum}\{ce_j\}}} \cdot \frac{\sum_{\forall m \in M_j} R_{fix} \cdot f_j(\gamma_m^{[t-1]})}{\sum_{m=1}^{|M|} R_{fix} \cdot f_j(\gamma_m^{[t-1]})}}{(M_j^{[t-1]})^2 \cdot \frac{\sum_{\forall m \in M_j} E_m^{[t-1]}}{\sum_{m=1}^{|M|} E_m^{[t-1]}}} \tag{4.4}$$

where ce_j denotes the coverage efficiency of protocol j:

$$ce_j = \frac{\frac{1}{M} \cdot \sum_{m=1}^{|M|} M_{reach,m}}{\sqrt{\pi \cdot d_{range,j}^2}} \tag{4.5}$$

with $M_{reach,m}$ being the number of UEs accessible by UE m when operating under WNP j (within $d_{range,j}$). $M_j^{[t-1]}$ is the number of devices utilizing protocol j during the timeslot $[t-1]$, $\sum_{\forall m \in M_j} R_{fix} \cdot f_j(\gamma_m^{[t-1]})$ is the data rate achieved by all the UEs operating with protocol j during $[t-1]$, and $\sum_{m=1}^{|M|} R_{fix} \cdot f_j(\gamma_m^{[t-1]})$ is the overall achieved data rate during $[t-1]$. $\sum_{\forall m \in M_j} E_m^{[t-1]}$ is the energy consumed by all the UEs operating with protocol j during $[t-1]$, and $\sum_{m=1}^{|M|} E_m^{[t-1]}$ is the overall consumed energy during the $[t-1]$ timeslot.

For each UE-learning automaton m, we define an action probability vector $\mathbf{Pr_m}^{[t]} = \{Pr_{m,1}^{[t]}, ..., Pr_{m,j}^{[t]}, ...Pr_{m,|J|}^{[t]}\}$, where $Pr_{m,j}^{[t]}$ expresses the probability of UE m selecting the WNP j during the timeslot t. The action probabilities $Pr_{m,j}^{[t]}$ are updated following the learning automata model [208]. For an UE operating under protocol j, the probability of continuing on the same protocol is:

$$Pr_{m,j}^{[t]} = Pr_{m,j}^{[t-1]} + b \cdot r_j^{[t-1]} \cdot (1 - Pr_{m,j}^{[t-1]}) \tag{4.6}$$

while the probability of changing to a new protocol j' is:

$$Pr_{m,j'}^{[t]} = Pr_{m,j'}^{[t-1]} - b \cdot r_j^{[t-1]} \cdot Pr_{m,j'}^{[t-1]}, j' \neq j \tag{4.7}$$

where b is a step size parameter that controls the convergence speed of the learning process. The action probabilities eventually converge to a single operating WNP for every UE [208]. The final protocol distribution among UEs manages to consider the uniqueness of the given environment (users' positions and density), the mode-wise battery-life and achievable data

rate of the UEs. It can be easily shown that the complexity of the software-defined WNP selection process is $O(2|J||M|)$.

4.4 Context-aware Coalition Formation

A context-aware UE coalitions formation procedure is proposed based on the Chinese Restaurant Process (CRP) [109] considering both the physical distance and communication interest among UEs. The purpose is to create coalitions consisting of UEs with high communication interests and small distances among each other in order to: a) improve the energy-efficiency of the communication among the UEs via exploiting UEs' socio-physical characteristics; b) conclude to fewer transmissions to the DA, and c) decrease the PSN's congestion. To achieve this, we extend the classic CRP defining an interest-distance-dependent CRP (IDD-CRP).

To capture the socio-physical relations among the UEs, we define two graphs based on distance, $G^D = \{v, \epsilon^D\}$ and interest, $G^I = \{v, \epsilon^I\}$. The vertex set v is the set of UEs and the edges $\epsilon^{D/I} = \{\epsilon^{D/I}_{m,m'} \forall m, m' \in v\}$ represent the D2D distance $\epsilon^D_{m,m'} = d(m, m')$, where $d(m, m') \in [0, 1]$ is the normalized physical distance between m and m' and the D2D communication interest levels $\epsilon^I_{m,m'} = i(m, m')$, where $i(m, m') \in [0, 1]$ is their level of communication interest.

According to the IDD-CRP, a user m is connected with a user m' with a probability proportional to a decay function $g(\cdot)$ of their respective combined socio-physical distances or is unconnected and creates a new coalition with a probability proportional to a scalar parameter a that can directly influence the number of coalitions. All interconnected users form a single coalition c. We define the IDD-CRP decay function between UEs operating under the same protocol j as:

$$g(IDD(m, m')) = \begin{cases} 0, & if\ d_{m,m'} < d_{range,j},\ \forall m \in M_c \\ w_D D(m, m') + w_I ID(m, m'),\ otherwise \end{cases} \tag{4.8}$$

where M_c expresses the set of coalition's c members and $D(m, m') = -log_2(d(m, m'))$, $ID(m, m') = -log_2(1 - i(m, m'))$, with $w_I, w_D, w_D + w_I = 1$ being weights expressing the

importance of the interest and physical distance levels. Note that the first case of $g(\cdot)$ can be ignored in the case of a WNP j-agnostic coalitions formation. The IDD-CRP clusters a UE m to a UE m' with a probability:

$$P(m,m') = \begin{cases} \frac{g(IDD(m,m'))}{\sum_{m \neq m'} g(IDD(m,m'))+a}, & m \neq m' \\ \frac{a}{\sum_{m \neq m'} g(IDD(m,m'))+a}, & m = m' \end{cases} \tag{4.9}$$

The coalitions creation complexity is $O(|M|^2 + |M|(|M|-1))$.

The coalition head ch_c is selected based on its physical distance, its energy availability, and the communication interest with the other UEs. We introduce a combined interest-distance graph $G^{IDD} = \{v, \epsilon^{IDD}\}$, where $v = M_c$ and ϵ^{IDD} is the edge between members. Each UE's edge has a weight

$$w(m,m') = w_D \frac{D_0}{D(m,m')} + w_I \frac{ID_0}{ID(m,m')} \tag{4.10}$$

with D_0, ID_0 being the maximum values of the physical and interest distances.

The ch_c of coalition c becomes the UE m that maximizes an overall metric defined as:

$$score(m) = w_{cc}\, CC_{IDD}(m) + w_E \frac{E_0}{E_m}, \tag{4.11}$$

$$CC_{IDD}(m) = \sum_{\substack{m \in M_c \\ m \neq m'}} \left[\frac{sp(m,m')}{|M_c|-1} \right]^{-1} \tag{4.12}$$

where $CC_{IDD}(m)$ is a closeness centrality metric with $sp(m,m')$ being the overall edge weight of the shortest path between m, m' UEs. The weights w_{cc} and w_E can be properly defined to reflect the tradeoff and importance of the metrics of closeness centrality and energy availability. E_m denotes UE's m energy availability, and $E_0 = \max_{m \in M_c}\{E_m\}$. The complexity of the coalition head selection for all the coalitions is $O(|C|[(|M_c| + \frac{|M_c|(|M_c|-1)}{2}) + (|M_c|\frac{|M_c|(|M_c|-1)}{2} + |M_c|) + |M_c| log |M_c|])$.

4.5 User-centric Resource Management

Following the previous analysis, we introduce a resource management process to determine the optimal uplink transmission power P_m of each UE m in order to fulfill its QoS prerequisites (maximize the perceived satisfaction while operating in a PS-environment) after the WNP selection and the coalition formation is realized. The concept of the utility function is adopted to uniformly express these diverse QoS prerequisites with each UE m adopting a continuous and differentiable with respect to P_m utility function formulated as:

$$U_m(P_m) = \frac{R_{fix} \cdot f_j(\gamma_m)}{P_m} \tag{4.13}$$

where $R_{fix} \cdot f_j(\gamma_m)$ denotes the UE's achievable data rate when operating under protocol j (see Sections 4.2, 4.3).

Each UE aims to maximize its utility through the appropriate strategy for P_m. For each UE we formulate the following distributed utility maximization problem:

$$\begin{aligned} &\max_{P_m \in A_m} U_m(P_m, \mathbf{P_{-m}}) \\ &s.t.\ 0 < P_m \leq P_m^{Max} \end{aligned} \tag{4.14}$$

where $\mathbf{P_{-m}}$ is the uplink transmission power vector of the rest UEs, and $A_m = (0, P_m^{Max}]$ is the UE's m strategy space. This maximization problem is confronted as a non-cooperative game $G = [M, \{A_m\}, \{U_m\}]$, where its solution concludes to a stable operation of the system, following each UE's m individual decisions, and given the respective decisions of the rest UEs. A Nash Equilibrium (NE) point of the game G is a vector of UEs' uplink transmission powers $\mathbf{P}^* = [P_1^*, ..., P_m^*, ..., P_{|M|}^*]^T \in A$, with $A = A_1 \times \cdots \times A_{|M|}$ being the strategy set, where no UE has the incentive to change its strategy given the strategies of the rest of the UEs.

Definition 1. *A power vector* $\mathbf{P}^* = [P_1^*, ..., P_m^*, ..., P_{|M|}^*]^T$ *in the strategy set* A *is a Nash equilibrium of the game* $G = [M, \{A_m\}, \{U_m\}]$ *if the following condition* $U_m(P_m^*, \mathbf{P}_{\mathbf{-m}}^*) \geq U_m(P_m, \mathbf{P}_{\mathbf{-m}}^*)$, *holds true for every UE* m, *and for all* $P_m^* \in A_m$.

Theorem 1. *The non-cooperative power control game* G *has a unique NE point* $\mathbf{P}^* = [P_1^*, ..., P_m^*,$

$..., P^*_{|M|}]^T$, *where*

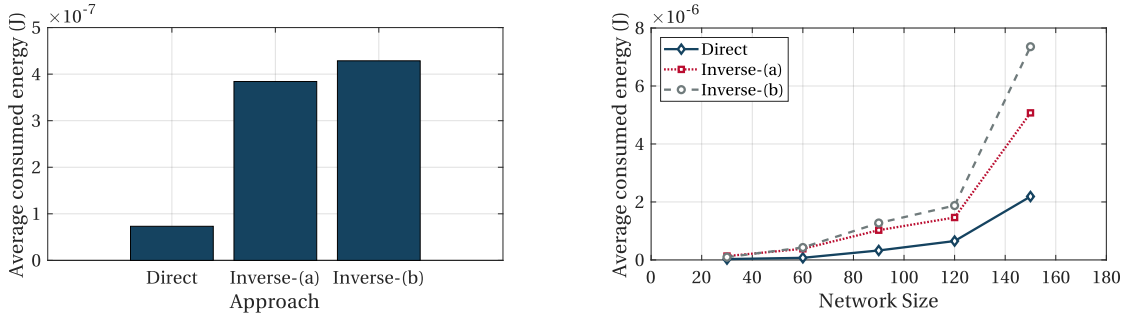
$$P^*_m(d_{m,m'}) = min\left\{\frac{\gamma^*_m I_m}{W G_{m,m'}}, P^{Max}_m\right\} \tag{4.15}$$

for all m, $m \in M$, *with* γ^*_m *being the unique positive solution of the equation* $\frac{\partial f_m(\gamma_m)}{\partial \gamma_m}\gamma_m - f_m(\gamma_m) = 0$.

The proof of this theorem is similar to the one found in [307]. The Nash equilibrium point determined by Eq. 4.15 can be interpreted as follows: given the strategies of the rest UEs, no independent UE has the incentive to chose a different strategy, as this would not improve its personal utility. In addition, due to the fact that the Nash equilibrium point exists, the stable outcome of the non-cooperative game G is guaranteed. The complexity of the user-centric resource management is $O(I[|M|(|M|+1)log(|M|+1)+|M|^2+l|M|])$, where I is the total number of iterations that the user-centric management framework needs to converge and l is the number of operations to determine each UE's power level per iteration.

4.6 Performance Evaluation

In this section, a detailed numerical evaluation of the proposed framework is conducted, in terms of its operation and performance. A wireless PSN NOMA setting is considered with $|M| = 60$ UEs randomly distributed in a $150m \times 150m$ area, with the DA located at the area's center. Each UE is able to utilize $|J| = 3$ protocols with transmission ranges equal to $d_{range,A/B/C} = [40\ 100\ 900]m$, and each timeslot is set at 0.5 $msec$. The background noise is $I_0 = 5 \cdot 10^{-15}$, while the desired transmission rate is assumed $R_{fix} = 256kbps$. IDD-CRP's parameter a is $a = 2$, the clustering weights are set to $w_D = w_I = 0.5$, $w_{CC} = w_E = 0.5$, and parameter $b = 0.7$. To express the coalition-head-to-DA (ch2DA) transmission load correlation with the communication interest among its members, we utilize an indicative normalized Interest-based Aggregation Factor (IAF) for each coalition $IAF_c = |M_c| - \sum_{m \in M_c, m \neq ch_c} i(m, ch_c)$. The latter represents the interest of the $|M_c|$ UEs to communicate with their ch_c, where a small value of IAF_c reflects the increased communication interest between the members and the ch_c. For each timeslot given the IAF_c value, the ch_c performs $1 + |IAF_c|$ transmissions to the DA.



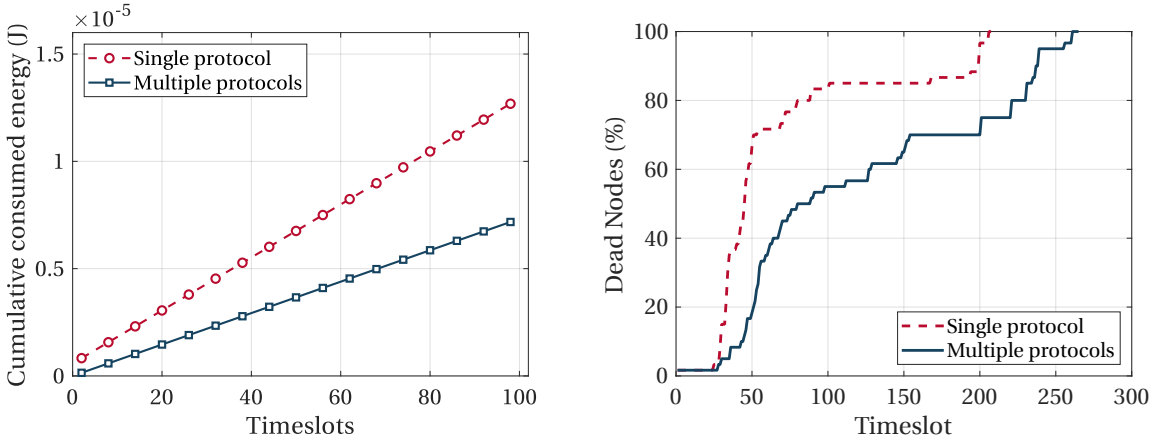
(a) Average consumed energy per approach **(b)** Consumed energy vs PSN size

Figure 4.2 Direct vs Inverse Operation Comparison

4.6.1 Direct vs Inverse Operation Comparison

For the overall framework operation, we examine two approaches: direct and inverse. In the direct approach, the UEs initially perform the WNP selection, and then, the UEs of the same protocol participate in a separate IDD-CRP coalition formation procedure resulting in same-protocol coalitions. For the inverse approach, the UEs perform a protocol-agnostic IDD-CRP coalition formation process. Then, all UEs participate in the WNP selection process and for their final protocol decision we examine two cases: (a) all coalition members adopt the coalition-head's protocol or (b) the protocol of the whole coalition is the one selected by the members' majority. For both approaches (i.e., direct and inverse), UEs follow the power allocation mechanism and decide their optimal uplink transmission powers.

Initially, we compare the operation alternative approaches in terms of energy consumption. Fig. 4.2a shows the mean PSN consumed energy as averaged over 100 timeslots after the convergence of the WNP selection process. In Fig. 4.2b, the average energy consumption is studied as a function of the PSN size. Both figures reveal the same trend with the direct approach outperforming the inverse ones since grouping already protocol-decided UEs leads to more efficient coalition formation and message bundling. Thus, for the following results, we focus on the direct operation approach.



(a) Consumed energy vs time

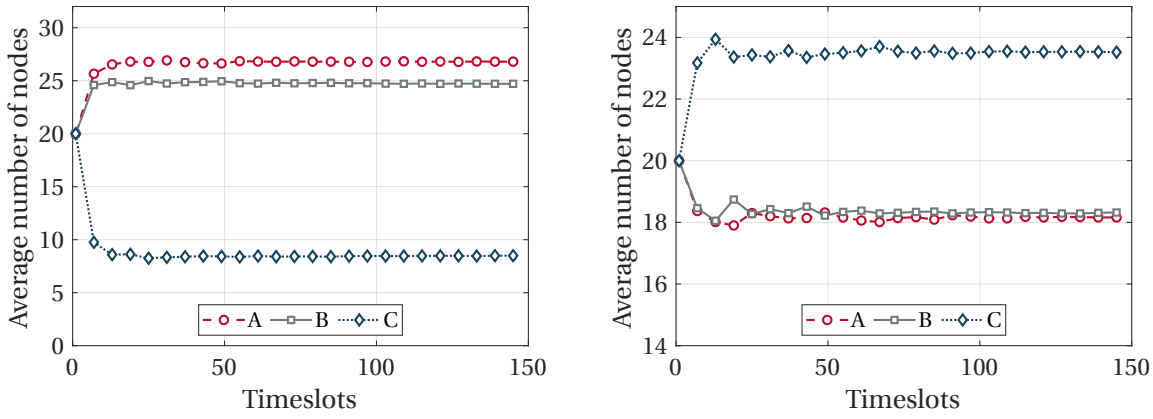
(b) Dead UEs vs time

Figure 4.3 Single vs Multiple Protocols Comparison

4.6.2 Single vs Multiple Protocols Comparison

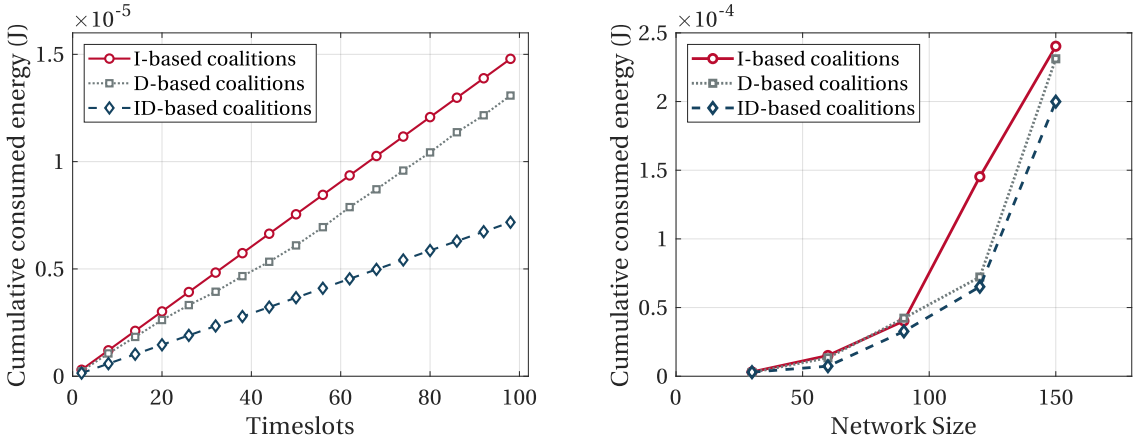
We compare the proposed multi-protocol PSN architecture with the single protocol approach that is nowadays coupled with the latest PSN additions of D2D communications and UE clustering [204]. For our case, we utilize the WNP with the largest range, as the single protocol to ensure communication among all UEs. Fig. 4.3a shows PSN's cumulative consumed energy as time evolves after the WNP selection convergence for the two discussed cases. With the heterogeneous PSN architecture, the energy consumption develops at a slower rate compared to the single WNP case. This pattern is further confirmed by Fig. 4.3b that depicts the percentage of UEs running out of energy as time evolves. For presentation purpose, the initial UEs' available energy is $E_m = 0.1\ \mu J$.

Given the benefits of the multi-protocol PSN architecture, we now focus on the ability of the WNP selection mechanism to adapt to diverse PSN topologies. We examine two scenarios, A and B, where $|M| = 60$ UEs are randomly placed in a $150m \times 150m$, and a $850m \times 850m$ area, respectively. We averaged the WNP distribution per timeslot for 500 different runs and random topologies. As shown in Fig. 4.4, Scenario A examines a dense PSN, thus the A and B protocols with the smaller range outweigh C, which is designed for long-range communications. The opposite is observed when a sparse topology is considered (scenario B), and the majority of UEs choose protocol C. The above observations confirm



(a) Scenario A **(b)** Scenario B

Figure 4.4 UEs' distribution per protocol j (A, B, C) per timeslot



(a) Consumed energy vs time **(b)** Consumed energy vs PSN size

Figure 4.5 Comparison of Coalition Formation Mechanisms

that the reward probability successfully adjusts the WNP distribution and prevents protocol starvation phenomena.

4.6.3 Comparison of Coalition Formation Mechanisms

Next, in order to quantify how coalition formation parameters affect the PSN energy efficiency, we compare three CRP-based coalition formation mechanisms: (a) ID-based:

considering jointly interest and distance among UEs as proposed here ($w_D = w_I = 0.5$), (b) I-based: considering exclusively communication interest among users ($w_D = 0$, $w_I = 1$), (c) D-based: considering only the distance among UEs ($w_D = 1$, $w_I = 0$). Fig. 4.5a presents the PSN's cumulative consumed energy due to UEs' transmissions as time evolves following the WNP selection process convergence, revealing how the combined context-aware coalition formation benefits the PSN energy consumption. In the I-based approach, the coalition contains UEs with high communication interest, but potentially deteriorated channel quality between them, thus the energy consumption burden is shifted to the coalition-members, which use higher transmission power to communicate successfully. On the contrary, in the D-based approach, the coalition contains UEs in close proximity with potentially low communication interest and force the ch_c to perform multiple transmissions to the DA (higher $|IAF_c|$) consuming more power. Therefore, the combined proposed approach is superior in terms of energy efficiency. Fig. 4.5b presents the same trend as the system's cumulative energy consumption at the 100^{th} timeslot after protocol convergence is studied as a function of the PSN size.

4.7 Related Work

In [339] the authors present a game-theoretic bandwidth allocation mechanism in heterogeneous wireless networks, where multi-mode UEs statically select and operate with different technologies (LTE, WiMAX, and WLAN). Each supported radio technology defines a different coverage area, thus creating a variety of service areas, while game theory is adopted to obtain the optimal bandwidth allocation per service area. In [204], the benefits of D2D communication are examined regarding the problem of homogeneous RF-based interference mitigation in PSN. Results identify a four-time increase in realistic conditions when D2D-based PSNs are compared with the regular LTE setting. In [190], the authors present a PSN model of a shared radio access network where shared cells, e.g., small cells, Unmanned Aerial Vehicles (UAV), are deployed on-command to fulfill PS-related network requirements including resilience, capacity, and coverage. The architecture provides reduced PSN deployment time, along with efficient and independent resource allocation between PS and commercial users. In [59] the authors propose a hybrid broadband PSN

architecture where stationary access points (APs) serve the routine PS traffic, while in case of emergency incidents dynamically deployed APs are dispatched to aid heavier PSN traffic needs. Finally, in [92] authors review the key challenges in D2D WNPs, identifying application possibilities and technical challenges regarding discovery and session establishment, resource allocation for QoS guarantee, interference management, and D2D multiple-input-multiple-output (MIMO) transmissions. Also, the authors analytically present and compare characteristics of short-range wireless transmission techniques.

4.8 Conclusion

In this chapter, we propose a heterogeneous PSN framework that exploits the multi-protocol capabilities of UEs to reduce transmission costs. A software-defined WNP selection is performed via a reinforcement learning technique considering the PSN environment, along with UEs QoS and available energy parameters. A context-aware CRP-based coalition formation is utilized to group PSN UEs by considering communication interest, physical distance, and UEs battery-life. To ensure an energy-efficient PSN, a distributed non-cooperative game-theoretic framework is introduced to determine UEs' equilibrium transmission powers. The framework was evaluated for its efficiency by studying various operation approaches and was compared against commonly used approaches.

Chapter 5

UAV-Aided Wirelessly Powered Public Safety Networks

A first version of this chapter was published in [266], and an extended version was originally published in [277].

5.1 Introduction

In this chapter, we consider the same setting as the previous chapter where a public safety network needs to be deployed in the smart city setting during an emergency and post-disaster scenario. In the previous chapter, we described the importance of a heterogeneous –in terms of utilized wireless interfaces– scheme to achieve an energy-efficient operation for the communication devices. In this chapter, we re-imagine the public safety network deployment in the heart of an IoT-equipped smart city, and consider the use of additional technologies –mobile UAV, and wireless charging– towards further extending the overall lifetime of the critical communication network.

As mentioned in chapter 4, the recent trend of mixed PSN designs that combine centralized communication and D2D connections can be further expanded by the increasing integration of Internet of Things (IoT) architectures in everyday life. Indeed, low-power sensing devices have started to actively coexist with traditional city or building infrastructures (e.g. streetlights [222]) as parts of various user-centric applications, such as user

tracking in smart facilities [260], user-health monitoring [135], or environmental sensing through multi-purpose IoT devices [274, 275]. This new reality motivates and demands the examination of traditional PSNs as part of a Public Safety IoT (PS-IoT) ecosystem, where the PSN is extended to include apart from user equipment devices (UEs), and first responder communication equipment, the plethora of IoT devices that exist in the disaster-struck PS-threatening area [276].

Until now the literature that examines the PSN and IoT architecture requirements (see Section 5.9 for details), mainly targets the following problems: (a) use of UAVs and their positioning, (b) efficient resource management, and (c) optimal D2D communication establishment between the IoT nodes. However, such research efforts [159, 207, 220, 233, 256, 323] have confronted each research pillar ((a)-(c)) in an isolated or pair-wise manner. Thus, the establishment of a holistic approach for studying the overall operation of wireless powered UAV-assisted PS-IoT remains a challenging research gap. More importantly, due to the existing critical conditions in PSNs and the expected unavailability of centralized cellular solutions, it is of paramount importance to devise distributed, autonomous, and resilient alternative communication paradigms.

Our work aims exactly at filling this gap and proposes a holistic distributed approach where the PS-IoT-nodes can operate in an autonomous manner targeting the energy-efficient communication in a UAV-assisted Wireless Powered non-orthogonal multiple access (NOMA) PSN. The proposed mechanism, where each node can transmit information either to the UAV/eNB (Device-to-eNB: D2eNB) or to another IoT node (D2D), revolves around two main elements. Since within a PSN, all the nodes may not be characterized by the same communication or power capabilities, some critical nodes may be able to assist the rest via acting as emergency gateways and forwarding the collected data to the mobile UAV. Thus, the critical PS-IoT nodes may act for example as coalition heads (chs), while the rest of the UEs act as coalition members. The first component exploits the notion of reinforcement learning to enable the self-adaptive behavior of each node towards determining its role (member/ch) within the PS environment and their D2D affiliations (self-adaptive coalition formation). The second one builds on those relationships to introduce a resource management mechanism for a UAV-assisted WPC architecture, where the UAV is the single energy source and the harvest-transmit-store model is adopted by the IoT nodes. The proposed solution aims to jointly optimize the IoT-nodes' uplink power control and dictate

an energy-efficient UAV trajectory. The two key research thrusts mentioned above can be decomposed into the following main contributions of this chapter, as summarized below:

- A distributed game-theoretic PS-IoT devices' role selection mechanism is introduced allowing the nodes to dynamically and in a distributed fashion, choose their role (i.e., coalition head or coalition member). We model the problem as a Minority Game and confront it using a machine learning technique (Sections 5.1 and 5.2).
- A reinforcement learning-based coalition formation mechanism among nodes is then adopted. Member nodes acting as stochastic learning automata select their coalition head considering their physical proximity and the coalition head's energy availability (Section 6).
- A UAV-assisted WPC model is used where the UAV is responsible for charging the PS-IoT nodes. The WPC phases occur within the same timeslot where the PS-IoT devices operate in a harvest-transmit-store fashion (Section 3).
- A distributed resource management mechanism is proposed that jointly optimizes the PS-IoT devices' uplink transmission powers and dictates the UAV positioning considering its speed constraints. Specifically, the optimal transmission power (unique Nash equilibrium) of each node is obtained through a non-cooperative game-theoretic approach, under the consideration of a distributed maximization problem of each node's utility function capturing its Quality of Service (QoS) prerequisites (Section 4.2). The problem of UAV optimal positioning in a Euclidean 3D space is formulated as a maximization problem of the energy availability of the coalition head nodes, being the ones that have the most critical role within the PSN, acting as emergency gateways (Section 4.1).
- Detailed numerical and comparative results demonstrate that the proposed holistic framework concludes to a promising solution for realizing energy-efficient self-adaptive PSNs (Section 8).

The remaining of this chapter is organized as follows. Section 5.2 describes the operation framework outline, while section 5.3 presents the PSN system model. Section 5.4 presents

and solves the energy-efficient uplink power allocation problem and describes the mobile UAV positioning mechanism. The autonomous PS-IoT devices' role selection process is presented in Section 5.5, while the reinforcement learning-based coalition formation process is detailed in Section 5.6. Section 5.7 presents in detail the overall framework's operation and flow of computation tasks. Finally, a detailed numerical and comparative evaluation of the proposed framework is provided in Section 5.8. Section 5.9 details the related literature, while Section 5.10 concludes the chapter.

5.2 Framework Overview

In this section, we provide a brief overview of the overall framework's operation as seen in Fig. 5.1 and present the wireless powered communication model. Additional details and models concerning each element of the overall framework, are provided in the subsequent sections. By utilizing an autonomous decision mechanism based on the Minority Game [236], each PS-IoT device selects its role inside the PS-environment, namely to become a simple coalition member or an emergency gateway coalition head (ch). The node role selection marks the initialization of a UAV relocation period with a length of T timeslots. At the beginning of each timeslot, the member nodes act as stochastic learning automata and select a coalition head to transmit their data, based on a reward probability ($r_{m,c}$) value associated with each coalition head (ch). The selection takes into account each node's previous choices, the ch's energy availability, and the PSN topology. Eventually, the learning process converges, that is each member constantly selects the same ch and becomes a permanent member of the coalition, and thus the number ($|M_c|$) and set (M_c) of nodes per coalition is determined. Following that, all nodes harvest energy from the UAV's downlink transmission and send their data in the uplink (member-to-ch and ch-to-UAV transmissions) as shown in Fig. 5.2. The optimal uplink transmission power is determined through a distributed resource management mechanism, and the UAV determines its upcoming position (next timeslot) considering the longevity of the emergency gateway coalition heads. Eventually, the location of the UAV stabilizes when the location update is below a certain distance threshold (see Section 5.4), with the UAV hovering in its converged position until the end of the period T. During each relocation period, the UAV moves to

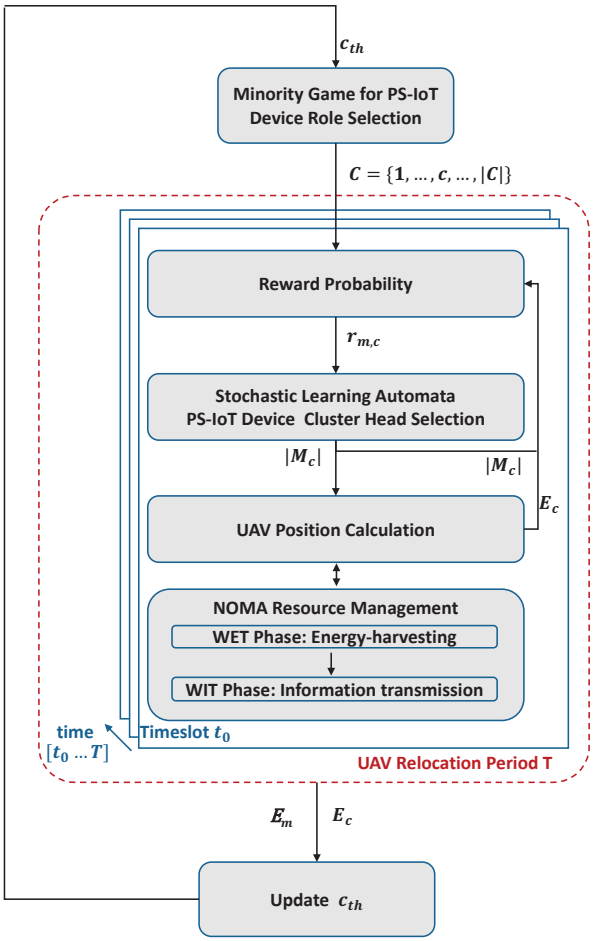


Figure 5.1 General Framework

support primarily the emergency gateway chs' operation. Thus, in an attempt to provide support to the PSN as a whole, the UAV relocation period T is periodically repeated, by updating the number of coalition heads according to the real public safety needs (see Section 5.5) and repeating the role selection process that will probably yield a new set of emergency gateway coalition heads.

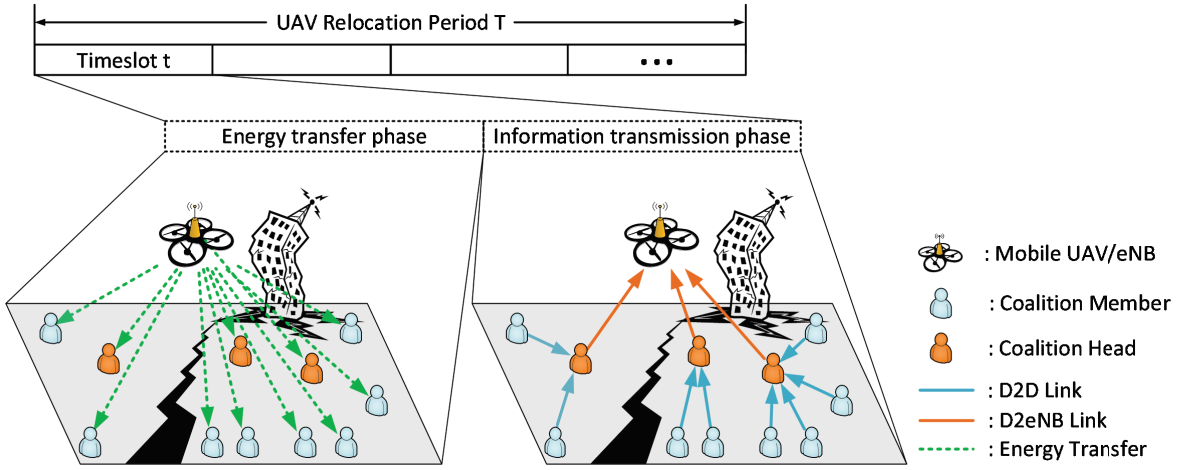


Figure 5.2 Public Safety Network topology

5.3 System Model

We consider the uplink channel of a NOMA wireless PSN that consists of $|M|$ PS-IoT devices, whose set is denoted by $M = \{1, ..., m, ..., |M|\}$, and they are served by a UAV-based evolved Node B (eNB). The PSN is deployed on a $l \times l$ square critical area with the coordinates of each device m denoted by $\{x_m, y_m, z_m\}$, and those of the UAV by $\{x_{UAV}, y_{UAV}, z_{UAV}\}$. In the rest of the chapter, the terms PS-IoT devices and nodes will be interchangeably used to describe the existing devices in a PSN, namely sensors, UEs, first responder equipment, etc. The PS-IoT devices are assumed to be identical regarding their characteristics with each one being able to harvest energy following the WPC technique. In the following, the wireless energy transfer phase will be denoted as WET, and the wireless information transmission phase as WIT. Each node can interchange between a WIT and WET phase during each timeslot, and additionally store harvested energy leftovers for future use (harvest-transmit-store model, see Section 5.2). Regarding the transmission capabilities during the WIT phase, as mentioned above, two possible communication types are considered: (a) D2D - direct node to node communication, (b) D2eNB - PS-IoT devices communicate directly with the mobile UAV/eNB.

In addition, several PS-IoT devices will act as coalition heads and will be considered as critical nodes within the PSN. Those devices are in charge of acting as emergency gate-

ways, collecting the members' transmission data, and forward the information to the UAV-mounted eNB. Let us denote the set of these critical nodes as $C = \{1, ..., c, ..., |C|\}$. In Section 5.5, we explain in detail how the set of critical devices is identified among all the existing nodes. Each device m is associated exclusively to a coalition head c (belongs to a single coalition), while the set of nodes associated with a coalition is $M_c = \{1, ..., |M_c|\}$, with $|M_c|$ being its cardinality. Section 5.6 describes how each node autonomously chooses its coalition head, as well as its coalition. The aforementioned public safety network topology is illustrated in Fig. 5.2.

Regarding the adopted wireless channel modeling, we define the channel gain between the transmitter m and a receiver m' (either a ch or the UAV) as:

$$G_{m,m'} = \frac{K}{d_{m,m'}^2} \tag{5.1}$$

where K is a positive constant that expresses the channel fading and $d_{m,m'}$ is the Euclidean distance between nodes m and m'. Since the PSN operates in a NOMA setting due to the Successive Interference Cancellation (SIC) technique [184], the channel gains observed by node m (receiver) are sorted as $G_{|M|,m} \leq ... \leq G_{m',m} \leq ... \leq G_{1,m}$ with the sensed interference of the node m given by:

$$I_m(\mathbf{P_{-m}}) = \sum_{m' \geq m+1}^{|M|} G_{m',m} P_{m'} + I_0 \tag{5.2}$$

where I_0 denotes thermal noise and $\mathbf{P_{-m}}$ is the uplink transmission power vector of the rest IoT devices excluding device m. Finally, the m^{th} node's signal-to-interference-plus-noise-ratio (SINR) towards a receiver m' is given by:

$$\gamma_m(P_m, \mathbf{P_{-m}}) = \frac{G_{m,m'} P_m}{I_{m'}} \tag{5.3}$$

with $I_{m'}$ being the receiver's sensed interference (Eq. 5.2) and P_m the device's uplink transmission power.

With respect to the WPC model [33], we adopt the harvest-transmit-store mechanism assuming that each PS-IoT device is equipped with a built-in rechargeable battery. Each timeslot t is divided into two phases, where initially the PS-IoT devices harvest energy from the broadcasted RF-signals (UAV's downlink transmission) for time τ_1 (WET phase).

Following that, each node transmits information for time τ_2 (WIT phase) with $t = \tau_1 + \tau_2$. For each member node, m and coalition head c the harvested energy is given by:

$$\begin{aligned} E_m^{har}(d_{m,UAV}) &= n\,\tau_1\,P_{UAV}\,G_{UAV,m} \\ E_c^{har}(d_{c,UAV}) &= n\,\tau_1\,P_{UAV}\,G_{UAV,c} \end{aligned} \tag{5.4}$$

where:

- $G_{UAV,m}$ and $G_{UAV,c}$ are obtained according to Eq. 5.1
- $n \in (0,1]$ is the energy efficiency conversion factor that depends on the receiver's hardware specifications
- $d_{m,UAV}$ is the euclidean distance between node m and the UAV given by $d_{m,UAV} = \sqrt{(x_{UAV}-x_m)^2+(y_{UAV}-y_m)^2+(z_{UAV}-z_m)^2}$ (same reasoning for $d_{c,UAV}$)
- P_{UAV} is the downlink transmission power of the UAV.

We denote the pre-existing energy availability of each coalition head and coalition member at each time slot as E_c, and E_m respectively.

5.4 UAV Trajectory and Resource Management

5.4.1 Mobile UAV-mounted eNB Positioning

In this subsection, we focus on determining the specific trajectory of the UAV-based eNB given the speed constraints of the UAV and the duration of each timeslot. The key objective is to extend the energy availability of the critical gateway chs in order to make up for the increased power cost of the uplink transmissions towards the high altitude-places of the UAV. We will assume that the UAV's movement is analyzed as a uniform motion across each axis of the Euclidean 3D space with the constant velocity per axis denoted by (u_{UAV}^x, u_{UAV}^y, u_{UAV}^z). The proposed approach positions the UAV in an attempt to maximize the energy availability sum of the emergency gateway chs for each timeslot. The optimization problem is expressed

as:

$$\max_{\substack{x_{UAV}\\ y_{UAV}\\ z_{UAV}}} \sum_{\forall c \in C} (E_c^{[t-1]} + E_c^{har} - E_c^{tran}) \tag{5.5}$$

$$\begin{aligned} s.t.\, 0 \leq x_{UAV}^{[t-1]} - u_{UAV}^{x} \cdot t \leq x_{UAV} \leq x_{UAV}^{[t-1]} + u_{UAV}^{x} \cdot t \leq l \\ 0 \leq y_{UAV}^{[t-1]} - u_{UAV}^{y} \cdot t \leq y_{UAV} \leq y_{UAV}^{[t-1]} + u_{UAV}^{y} \cdot t \leq l \\ h_{min} \leq z_{UAV}^{[t-1]} - u_{UAV}^{z} \cdot t \leq z_{UAV} \leq z_{UAV}^{[t-1]} + u_{UAV}^{z} \cdot t \end{aligned}$$

where:

- $d_{c,UAV} = \sqrt{(x_{UAV} - x_c)^2 + (y_{UAV} - y_c)^2 + (z_{UAV} - z_c)^2}$, the euclidean UAV-ch c distance
- E_c^{har} the energy availability of the critical PS-IoT node c
- h_{min} the minimum allowed flight altitude of the UAV
- E_c^{tran} the energy spent due to the uplink transmission given by $E_c^{tran} = \tau_2 \cdot P_c^*(d_{c,UAV})$, where P_c^* is the optimal transmission power depending on the physical UAV-node c distance. The calculation of P_c^* is discussed in detail below.

Using Eq. 5.4 and with some simple derivations, the solution of the maximization problem (5.5) is given by:

$$(x_{UAV}^*, y_{UAV}^*, z_{UAV}^*) = \underset{\substack{x_{UAV}\\ y_{UAV}\\ z_{UAV}}}{arg\,max} \left[\sum_{\forall c \in C} E_c^{[t-1]} + \sum_{\forall c \in C} n\, \tau_1\, P_{UAV}\, G_{c,UAV} - \sum_{\forall c \in C} \tau_2 \cdot P_c^*(d_{c,UAV}) \right] \tag{5.6}$$

The UAV moves until the location updates at each timeslot become lower than a threshold (e.g., 10^{-2} meters), i.e., the UAV's position converges given the PS-environment and the current chs positions.

5.4.2 Uplink Transmit Power Management

To further support the energy efficient operation of PS-IoT devices, we aim at low nodes' transmission power levels. This is achieved through the formulation of a distributed resource management problem to calculate the optimal uplink transmission power P_m^* of each node (both coalition head and member) to maximize its perceived satisfaction and

fulfill its QoS prerequisites when operating within the challenging PS-critical environment. For this resource allocation mechanism, we adopt the concept of the utility function that uniformly expresses all the diverse PS-IoT devices' QoS prerequisites. Each node adopts a differentiable, and continuous utility function U_m with respect to its transmission power P_m [253], formulated as :

$$U_m(P_m) = \frac{W \cdot f_m(\gamma_m)}{P_m} \tag{5.7}$$

where:

- $f_m(\gamma_m)$ expresses the successfully transmitted bits between the transmitter m and the receiver (either another node or the UAV)
- W denotes the system's bandwidth.

The efficiency function $f_m(\gamma_m)$ is continuous, differentiable, and increasing with respect to γ_m (Eq. 5.3), having a sigmoidal-like shape, such that after a γ_m^{target} point, $f_m(\gamma_m)$ is concave, and below it is convex. Without loss of generality, as widely used in literature (e.g. [253], [179]), we adopt:

$$f_m(\gamma_m) = (1 - e^{-A\gamma_m})^M \tag{5.8}$$

on where A is a real valued positive parameter that controls the slope of the sigmoidal function and M denotes the transmitted packet size (in bits) [253]. Moreover, by controlling parameters A and M, f_m becomes flexible enough towards capturing user QoS prerequisites for diverse conditions and use cases within a deployed IoT-based PSN.

Considering the conditions under which the PSN is deployed, each node aims at maximizing its utility as defined in Eq. 5.7, through selecting an appropriate strategy for the uplink transmission power. Thus, for each UE we formulate the following distributed utility maximization problem:

$$\begin{aligned} &\max_{P_m \in A_m} U_m(P_m, \mathbf{P_{-m}}) \\ &s.t.\ 0 < P_m \leq P_m^{Max} \end{aligned} \tag{5.9}$$

where $A_m = (0, P_m^{Max}]$ is the strategy space of the PS-IoT device m, and $\mathbf{P_{-m}}$ is the uplink transmission power vector of the rest IoT nodes (excluding m). Regarding the uplink trans-

mission power P_m of each IoT node, it is bounded, i.e., $0 \leq P_m \leq P_m^{Max}$, and given the energy harvested during the WET phase of duration τ_1:

$$P_m^{Max}(d_{m,UAV}) = \frac{E_m + E_m^{har}}{\tau_2} = \frac{E_m + n \cdot \tau_1 \cdot P_{UAV} \cdot G_{m,UAV}}{\tau_2} \tag{5.10}$$

The utility maximization problem is confronted as a non-cooperative game $G = [M, \{A_m\}, \{U_m\}]$ among the PS-IoT nodes and its solution concludes to the optimal equilibrium for the PSN, following each node's m individual decision, and given the respective decisions of the rest IoT devices. A Nash equilibrium point of the game $G = [M, \{A_m\}, \{U_m\}]$ is a vector of nodes' uplink transmission powers $\mathbf{P}^* = [P_1^*, ..., P_m^*, ..., P_{|M|}^*]^T \in A$, where the strategy set is denoted as $A = A_1 \times ... \times A_m \times ... \times A_{|M|}$.

A power vector $\mathbf{P}^* = [P_1^*, ..., P_m^*, ..., P_{|M|}^*]^T$ in the strategy set $A = A_1 \times ... \times A_m \times ... \times A_{|M|}$ is a Nash equilibrium of the game $G = [M, \{A_m\}, \{U_m\}]$ if the following condition holds true:

$$U_m(P_m^*, \mathbf{P}_{-\mathbf{m}}^*) \geq U_m(P_m, \mathbf{P}_{-\mathbf{m}}^*) \tag{5.11}$$

for every IoT node m, and $\forall\ P_m^* \in A_m$.

Theorem 2. *The non-cooperative power control game $G = [M, \{A_m\}, \{U_m\}]$ has a unique Nash equilibrium point $\mathbf{P}^* = [P_1^*, ..., P_m^*, ..., P_{|M|}^*]^T$, where*

$$\begin{aligned} P_m^*(d_{m,c}) &= min\left\{\frac{\gamma_m^* I_m}{W G_{m,c}}, P_m^{Max}\right\},\ m \notin C \\ P_c^*(d_{c,UAV}) &= min\left\{\frac{\gamma_c^* I_c}{W G_{c,UAV}}, P_c^{Max}\right\} \end{aligned} \tag{5.12}$$

for all m, $m \in M$, with γ_m^* being the unique positive solution of the equation:

$$\frac{\partial f_m(\gamma_m)}{\partial \gamma_m}\gamma_m - f_m(\gamma_m) = 0 \tag{5.13}$$

The proof of the above theorem is concluded following similar steps as in the procedure described in [157]. The Nash equilibrium point determined by Eq. 5.12 can be interpreted as follows: given the strategies of the rest PS-IoT nodes, no independent node has the

incentive to chose a different strategy, as this would not improve its personal utility. In addition, due to the fact that the Nash equilibrium point exists, the stable outcome of the non-cooperative game G is guaranteed.

5.5 Autonomous PSN Coalition Head Role Selection

5.5.1 A Minority Game Approach

Apart from improving the PSN's energy autonomy, among our proposed framework's operational objectives is the autonomous behavior of the PS-IoT nodes. Towards this direction, we utilize a minority game-theoretic approach [54, 236] to model the PS-IoT devices' role selection process and utilize machine learning for its solution. The minority games (MG) are used to model the interaction of autonomous agents competing for a shared resource. In the classic form of the game, an odd number of players repeatedly selects between two available strategies (e.g., be a coalition head or a coalition member), and the players compete with each other to be part of the minority group. The players/agents that belong to the minority group win and promote their winning action for the next round of the game. The winning action of the MG is globally announced by a central entity, which is not however responsible for taking any decisions regarding the game. Each player is agnostic of other players' strategies and makes an autonomous decision regarding his strategy based only on historical data of the consecutive game outcomes. The minority game has a non-empty set of pure Nash equilibria [54], and reinforcement learning algorithms (e.g., Q-learning, exponential learning) are utilized to implement each agent's learning process [50].

In this work, we will utilize a generalized version of the MG (minority game with arbitrary cut-offs [149]) where the minority is defined by a specific cut-off value. In the following let us denote the game as $G_{MG} = [M, \{A_m\}, \{R_{a_m}(m)\}]$, where M is the set of odd agents, i.e., PS-IoT devices, $A_m = 0, 1$ is the set of strategies, i.e., roles, and $R_{a_m} : \{1, ..., m, ..., |M|\} \longrightarrow \mathbb{R}$ for each $m, m \in M$ is the reward that each PS-IoT node m receives after selecting a strategy/role. We denote the strategies for each PS-IoT node during each MG round i as a_m, $a_m \in A_m$, and each device can choose between two possible actions, namely $a_m^{[i]} = 0$ to become coalition member, and $a_m^{[i]} = 1$ to become coalition head. The collective sum of IoT nodes' MG actions is referred to as attendance c_i for round i and in our case is equal to the number of coalition

heads (i.e., the minority group). The cut-off value c_{th} expresses a limit on the number of PSN chs.

In our game model, we consider the location of the UAV as the PS-IoT devices' shared resource. This is motivated by the fact that the movement and the position of the UAV is obtained by taking into account only the chs' energy availability (as discussed in Section 5.4), since only the chs (i.e., critical emergency gateway IoT nodes) transmit information to the UAV, on behalf of the rest of the members. If $c^{[i]} \leq c_{th}$, the $c^{[i]}$ chs are considered as winners earning a unit reward, while if $c^{[i]} \geq c_{th}$, the members are considered to be the minority game's winners as the increased number of chs leads to poor UAV positioning and therefore smaller energy efficiency rewards for them. The game is repeated for each round i with each node m initially taking an action $a_m^{[i]}$. Following the independent nodes' actions the UAV (central MG entity) broadcasts the winning choice b to all participants, i.e., $b^{[i]} = 1, \ if \ c^{[i]} \leq c_{th}$ or $b^{[i]} = 0, \ otherwise$. It is noted that the final decision of the role selection is taken by the IoT devices in an autonomous manner. The received payoff ($R_{a_m}(m)$) of node m after its strategy/role selection, i.e., a_m, at the MG's round i, i.e., $R_{a_m}^{[i]}(m)$ is given as:

$$
\begin{aligned}
R_{a_m=1}^{[i]}(m) &= \begin{cases} 1, \ if \ c^{[i]} \leq c_{th} \\ 0, \ otherwise \end{cases} \\
R_{a_m=0}^{[i]}(m) &= \begin{cases} 1, \ if \ c^{[i]} > c_{th} \\ 0, \ otherwise \end{cases}
\end{aligned}
\tag{5.14}
$$

Concerning the cut-off value c_{th} that denotes the threshold number of coalition heads that the PSN demands, it is computed and updated at the end of each UAV relocation period. Since our aim for the coalition heads is to enjoy superior payoffs than costs to be able to act as emergency gateways and broadcast their member data, we want a ch-related payoff to be greater than a member-associated payoff. By expressing this reward as the average

energy availability of each group at the end of each UAV relocation period T we get:

$$\frac{\sum\limits_{\forall c\in C} E_c^{[T]}}{|C|} \geq \frac{\sum\limits_{\forall m\notin C} E_m^{[T]}}{|M|-|C|} \Rightarrow |C| \leq \frac{|M|\cdot \sum\limits_{\forall c\in C} E_c^{[T]}}{\sum\limits_{\forall c\in C} E_c^{[T]} + \sum\limits_{\forall m\notin C} E_m^{[T]}} \Rightarrow$$

$$|C| \leq \frac{|M|\cdot \sum\limits_{\forall c\in C} (E_c + (\sum\limits_{t=t_0}^{T} E_c^{har[t]} - E_c^{tran[t]}))}{\sum\limits_{\forall c\in C} (E_c + (\sum\limits_{t=t_0}^{T} E_c^{har[t]} - E_c^{tran[t]})) + \sum\limits_{\forall m\notin C} (E_m + (\sum\limits_{t=t_0}^{T} E_m^{har[t]} - E_m^{tran[t]}))} \tag{5.15}$$

Thus, the c_{th} value is updated as:

$$c_{th} = \left\lfloor \frac{|M|\cdot \sum\limits_{\forall c\in C} (E_c + (\sum\limits_{t=t_0}^{T} E_c^{har[t]} - E_c^{tran[t]}))}{\sum\limits_{\forall c\in C} (E_c + (\sum\limits_{t=t_0}^{T} E_c^{har[t]} - E_c^{tran[t]})) + \sum\limits_{\forall m\notin C} (E_m + (\sum\limits_{t=t_0}^{T} E_m^{har[t]} - E_m^{tran[t]}))} \right\rfloor \tag{5.16}$$

5.5.2 Machine Learning for Autonomous Role Selection

In order to determine the pure Nash equilibrium (NE) of the minority game G_{MG}, we propose a distributed learning algorithm that enables PS-IoT devices to act as sophisticated players and learn from their previous strategies towards selecting the most beneficial action at the upcoming game round. In this work, the distributed learning algorithm is adopted to solve the game and enable the PS-IoT devices to converge to one of the $\binom{M}{\frac{M-1}{2}} + \binom{M}{\frac{M+1}{2}}$ pure strategy NE [54]. According to the algorithm each node/player chooses a strategy a_m^i at each iteration round i with a probability $prob_{m,a_m}^i$ given by:

$$prob_{m,a_m}^i = \frac{e^{\kappa_m \pi_{m,a_m}^{[i]}}}{\sum\limits_{\forall a_m\in A_m} e^{\kappa_m \pi_{m,a_m}^{[i]}}} \tag{5.17}$$

where:

Algorithm 2 : Distributed Learning Algorithm for PS-IoT device role selection Minority Games

Input: c_{th}

Output: Set of coalition heads $C = \{1, ..., c, ..., |C|\}$

Initialization : Set $i = 1$, $\pi^{[i]}_{m,a_m} = 0$, $prob^{[i]}_{m,a_m} = 0.5$, $\forall m \in M, \forall a_m \in A_m$

while $not\ converged$ **do**

(a) PS-IoT devices select their action a_m

$$a^{[i]}_m = \begin{cases} 0,\ with\ probability\ prob^{[i]}_{m,a_m=0} \\ 1,\ with\ probability\ prob^{[i]}_{m,a_m=1} \end{cases}$$

(b) UAV/eNB broadcasts MG winning result $b^{[i]}$

$$b^{[i]} = \begin{cases} 0,\ if\ c^{[i]} > c_{th} \\ 1,\ otherwise \end{cases}$$

(c) Update each IoT device's accumulating score as:

$$\pi^{[i+1]}_{m,a_m} = \begin{cases} \pi^{[i]}_{m,a_m} + 1,\ if\ a^{[i]}_m = b^{[i]} \\ \pi^{[i]}_{m,a_m},\ otherwise \end{cases}$$

(d) Update each IoT device's strategies' selection probabilities as:

$$prob^{i+1}_{m,a_m} = \frac{e^{\kappa_m \pi^{[i+1]}_{m,a_m}}}{\sum\limits_{\forall a_m \in A_m} e^{\kappa_m \pi^{[i+1]}_{m,a_m}}}$$

(e) Check convergence criterion:

if $\forall m \in M\ \exists\ a_m \in A_m : |1 - prob^{i}_{m,a_m}| \leq \epsilon,\ \epsilon \to 0$ **then**

Convergence criterion met

else

$i = i + 1$

end if

end while

Return the set of UEs that selected a ch role (Set C)

- $\pi^{[i]}_{m,a_m}$ denotes the accumulated score of the strategy $a^{[i]}_m$. The score is increased in each round i only if the node's selected strategy is the one that won, i.e., $a^{[i]}_m = b^{[i]}$.
- $\kappa_m, \kappa_m \in \mathbb{N}$ expresses the learning rate of each IoT device m. For large κ values each IoT node selects the action with the highest accumulated score, while for small values of κ, each device explores alternative strategies from the set A.

The learning procedure is summarized in Algorithm 1.

5.6 Reinforcement Learning-based Coalition Formation

Given the PS-IoT devices' role selection and the resulting set C of coalition heads, each member node $m \notin C$ acts as a stochastic learning automaton to associate with a respective ch c. The UAV creates a set of reward probabilities $\boldsymbol{r}_m = \{r_{m,1}, ..., r_{m,c}, ..., r_{m,|C|}\}$, $r_{m,c} \in [0,1]$ at the beginning of each time slot t for each UE $m, m \notin C$ and broadcasts them to the member PS-IoT devices. The reward probabilities reflect the competitiveness of each ch c as perceived from the member node m, $m \notin C$ and are given by:

$$r_{m,c}^{[t]} = \frac{r_{m,c}'^{[t]}}{\sum_{c=1}^{|C|} r_{m,c}'^{[t]}}, \quad r_{m,c}'^{[t]} = \frac{E_c^{[t-1]}}{|M_c|^{[t-1]} \cdot (d_{m,c})^2} \tag{5.18}$$

where $|M_c|^{[t-1]}$ the number of members already assigned to c, and $E_c^{[t-1]}$ is the energy availability of ch c during the previous timeslot.

Following that, we define the action probability $P\,r_{m,c}^{[t]}$ of node m to select c as its coalition head during timeslot t. The probabilities are updated according to the stochastic learning automata model [208]: for a PS-IoT node m currently associated with ch c the probability of selecting a new ch c' ($c' \in C, c' \neq c$) is:

$$P\,r_{m,c'}^{[t]} = P\,r_{m,c'}^{[t-1]} - b \cdot r_{m,c}^{[t-1]} \cdot P\,r_{m,c'}^{[t-1]} \tag{5.19}$$

and the probability of continuing transmitting to the same ch is calculated as:

$$P\,r_{m,c}^{[t]} = P\,r_{m,c}^{[t-1]} + b \cdot r_{m,c}^{[t-1]} \cdot (1 - P\,r_{m,c}^{[t-1]}) \tag{5.20}$$

where b expresses the mechanism's learning rate. The action probabilities converge to a single coalition head choice for every IoT node. Note that the final members' distribution among coalition heads due to the reward probability formula manages to consider each ch's energy availability, the specific ch-member physical proximity and finally prevents the creation of oversized coalitions (and in turn chs with zero node members). The latter would lead to non-energy efficient communication within the PSN IoT setting.

5.7 Framework's Operation and Flow

Following the aforementioned analysis and discussions, in this section, we summarize the overall framework's operation and flow in a step-wise manner.

1. (*Initialization*) At the beginning of the first timeslot, i.e., $t = 0$, set the cut-off value c_{th} to an initial value (e.g., 20% of the IoT node population), and perform the distributed learning algorithm for PS-IoT device role selection based on the Minority Games (Algorithm 1) to determine the coalition heads in the PSN network.

2. (*Ch Selection Initialization*) After the identities of the chs are determined set the initial coalition head selection probability $Pr_{m,c}^{[t=0]} = \frac{1}{|C|}, \forall m \in M,\ m \notin C$.

3. (*UAV Upcoming Position Calculation - WET Phase*) At the beginning of each timeslot t the UAV calculates its upcoming position $(x_{UAV}^*, y_{UAV}^*, z_{UAV}^*)$ given its speed constrains $(u_{UAV}^x, u_{UAV}^y, u_{UAV}^z)$ via equation (5.6) and transmits in the downlink with power P_{UAV}, while the PS-IoT nodes harvest energy.

4. (*Coalition Formation*) At each timeslot $t > 0$, each PS-IoT node chooses a coalition head to be associated with and send its data to, according to the node's action probability $Pr_{m,c}^{[t]}, \forall m \in M, \forall c \in C$.

5. (*Uplink Transmit Power Management - WIT Phase*) Given that all the PS-IoT nodes have chosen a coalition head to send their data, then they determine their uplink transmission power levels as follows.
   a) Set $i = 0$, where i denotes the iteration of the resource allocation part of the algorithm.
   b) Each IoT node determines its optimal uplink transmission power as detailed in equation (5.12),
   c) If $|P_m^{[i+1]} - P_m^{[i]}| \leq \epsilon$ (where ϵ is a small positive constant), the powers have converged and the non-cooperative game stops. Otherwise, return to step 5b.

6. (*Coalition Head Selection*) Given the optimal power allocation, the UAV measures the competitiveness of each ch in relation to each node m, namely the reward probability

$r_{m,c}^{[t]}$ (Eq. 5.18) and transmits the values to the nodes. Then each IoT node updates its ch selection probability vector using the rules (5.19), and (5.20), and update their coalition head selection accordingly.

7. (*MG-based Ch Identity Update*) If the current timeslot is less than the designated UAV relocation period T (i.e., $t < T$) then return to step 3. Otherwise, calculate a new c_{th} value, perform Algorithm 1 to elect an updated set of coalition heads and return to step 2.

At this point, we should clarify that the overall framework is of low computational complexity, as at each step the involved calculations are based on expressions of closed-form. The main convergence points (in terms of necessary timeslots) are associated with: (a) the action probabilities convergence (i.e., coalition formation convergence), (b) the UAV positioning convergence, and (c) the MG distributed learning algorithm convergence. These points are discussed in more detail, and respective convergence times are specifically shown in the following section of numerical results. Indeed, based on the obtained results it is argued and verified that the convergence of each procedure above is fast, while the overall framework requires a fairly small number of timeslots to converge to a stable outcome (see Section 5.8 for details).

5.8 Performance Evaluation

In this section, we present a detailed numerical evaluation of the proposed framework's performance, mainly concerning its operational features, the coalition formation methodology, and the UAV-assisted resource management process, via modeling and simulation. The presented performance evaluation is based on simulated data under the MATLAB simulation environment.

Our evaluation considers a $250m \times 250m$ square public safety area with $|M| = 51$ IoT devices operating under NOMA technology. The IoT nodes are distributed randomly in the 2D plane (x,y coordinates), while their altitude (z coordinate) also varies randomly between 0.5m and 1.5m. The system's bandwidth is set at $W = 10^6\,Hz$, the duration of each timeslot is $t = 5\,msec$, and the thermal background noise is $I_0 = 5 \cdot 10^{-15}$. The UAV's maximum

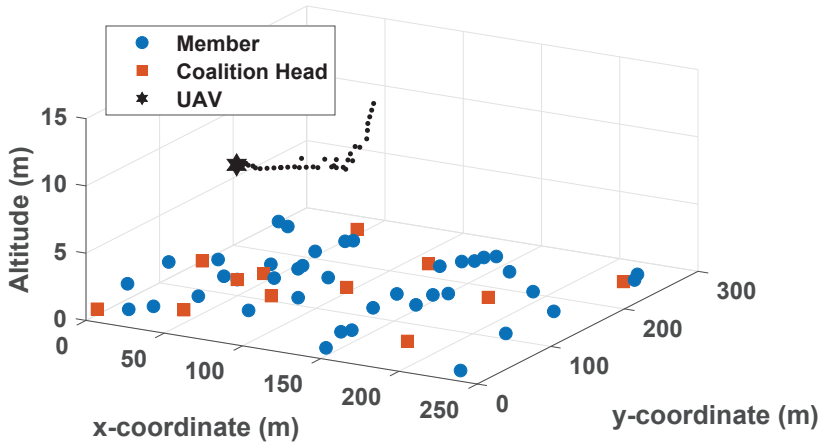


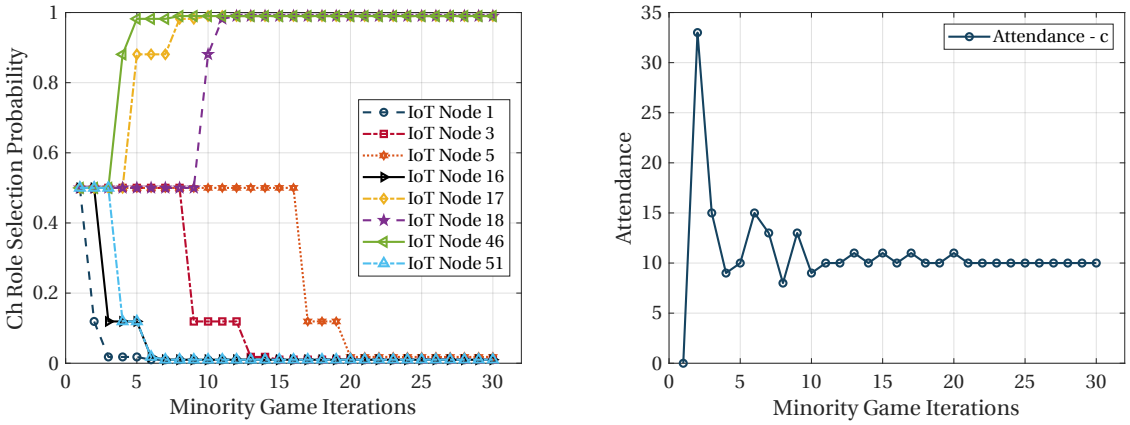
Figure 5.3 PSN topology and UAV's trajectory

velocity towards each axis of the 3D space is $\{u^x_{UAV}, u^y_{UAV}, u^z_{UAV}\} = \{50, 50, 50\}\, m/s$, and it is initially located at the center of the critical area with $\{x_{UAV}, y_{UAV}, z_{UAV}\} = \{125, 125, 15\}\, m$. Its minimum allowed flight altitude is set to $h_{min} = 10\, m$. Regarding the WPC related parameters, each timeslot is equally divided for the WET phase ($t_1 = t/2$) and the WIT phase ($t_2 = t/2$) implementation, while the downlink transmission power of the UAV is set to $P_{UAV} = 20$ dBm. The downlink transmission power was specifically chosen to not only match the uplink transmission power needs of the IoT devices but further charge them through the harvest-transmit-store WPC mechanism. Finally, the MG learning rate of each device κ is set equal to $\kappa_m = 2$.

A representative snapshot of the PSN topology and the UAV's trajectory, within a single relocation period T is depicted in Fig. 5.3. The UAV is initially positioned at the center of the critical 3D space and consecutively moves towards its final position. Taking into account practical restrictions regarding the UAV's speed, the figure also depicts its followed path, consisting of the optimal positions at each timeslot. Evidently, the coalition heads' locations heavily impact the UAV path formation and its final 3D placement.

5.8.1 Evaluation of Reinforcement Learning Components

Given this setting, we next evaluate the autonomous PS-IoT device role selection model, through the MG approach. Specifically, Fig. 5.4a presents the node's role selection proba-



(a) Convergence of IoT nodes' action probabilities **(b)** Convergence of IoT nodes' attendance c

Figure 5.4 Minority Game

bility for becoming a coalition head as a function of the distributed MG algorithm iterations (see Section 5.5). Evidently, the distributed learning algorithm for the minority game presents low convergence time, i.e., less than 20 iterations for all practical purposes, with each PS-IoT node selecting its role autonomously. Fig. 5.4b depicts the attendance for the same learning procedure, namely the number of coalition heads $|C|$, with the autonomous role selection concluding to an initially set threshold of $|c_{th}| = 10$, without any centralized decision making.

Next, we consider the impact of the learning automata parameter b on the action probabilities convergence speed and learning quality. Fig. 5.5 considers a specific IoT node topology and presents the number of timeslots required until all IoT member nodes converge to their respective ch choice. When large values of b are considered, the convergence time is lower with a reduction of 61.65% when moving from $b = 0.3$ to $b = 0.9$. However, it is generally accepted that for small b values the system concludes to more efficient and accurate choices [208], which in our case translates to more appropriate ch-member associations, and thus collectively lower transmission power vectors. In this context, Fig. 5.5 also presents the mean member-node energy consumption per timeslot, as averaged for 100 timeslots after the action probability convergence. It is observed that as b increases, so does the system's consumption due to the lower achieved quality with respect to the member-chs associations, and corresponding reduced coalition formation quality. For all

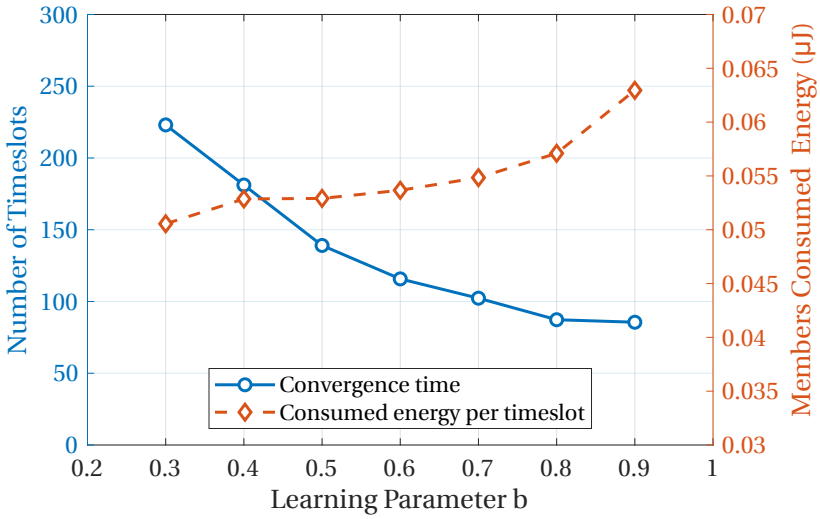


Figure 5.5 Coalition Formation - Impact of learning speed parameter b Study of the framework's reinforcement learning procedures and parameters

the following results we consider the learning automata parameter b equal to 0.7, which presents a well-balanced trade-off between convergence speed and obtained quality.

5.8.2 UAV Relocation Period Analysis and Evaluation

Next, we discuss the appropriate choice of the UAV relocation period duration T. As seen in Section 5.2 during a period T the member nodes converge to their optimal ch choices, and the UAV converges to an optimal location to efficiently charge the emergency gateway chs and collect the data. Moreover, for each new period, the set of coalition heads is renewed with nodes switching their role (from member to ch) due to the MG autonomous selection to enjoy increased support from the UAV as they join the minority group (see Section 5.5). Thus, the duration of T should account for both system needs mentioned above. To conclude to an appropriate T value for our setting, we considered a single topology and averaged 10 different runs for a total duration of 5000 timeslots. Five different cases were considered with the UAV relocation period being repeated 100, 50, 20, 10 and 5 times for T values of 50, 100, 250, 500, and 1000 timeslots respectively. Fig. 5.6 shows the energy availability of the PSN during the 5000 timeslot period. The total energy availability was

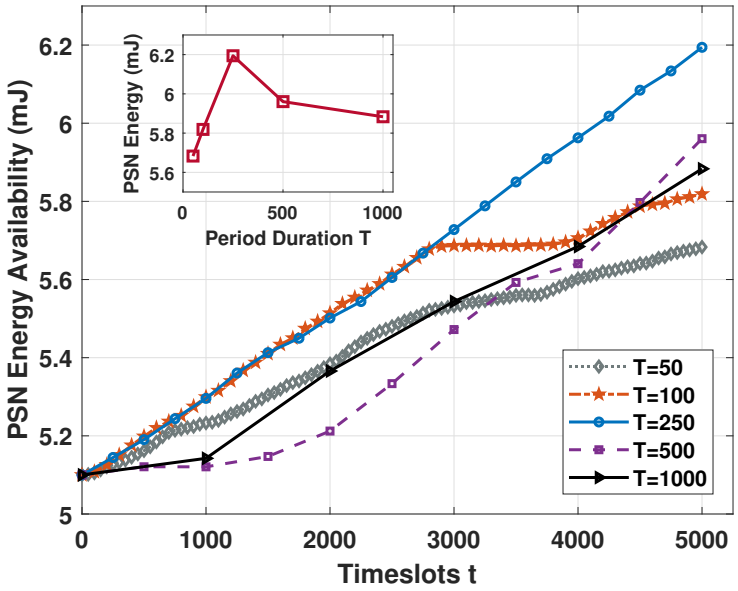
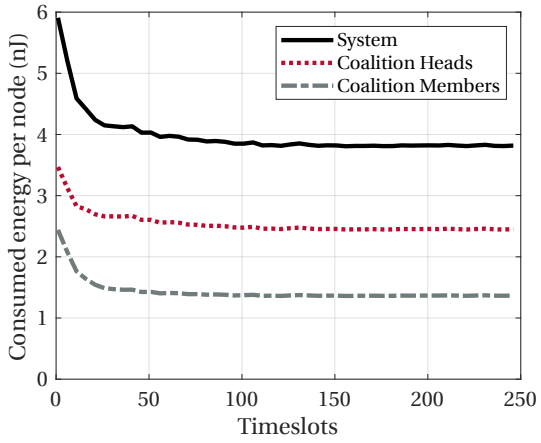


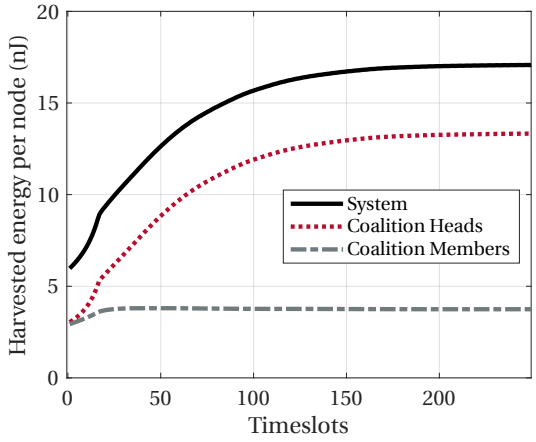
Figure 5.6 PSN energy availability for varying UAV relocation period duration

recorded after the end of each period T. Also, the total PSN energy availability after the 5000 timeslots run their course, as a function of period T, is also shown in Fig. 5.6 as a subfigure. Evidently, the use of a short UAV relocation period reduces the performance as the members have not concluded yet to the optimal ch choice, and the UAV either has not converged to its optimal location, or the hovering time above the critical nodes is limited. On the contrary, while long UAV relocation periods resolve the above issues, they do not allow for frequent role transitions, with fewer nodes acting as emergency gateway coalition heads during the 5000 timeslot period. Thus, a smaller subset of nodes gets to enjoy the increased ch benefits during the framework's operation. For all the following results we will consider a UAV relocation period $T = 250$ timeslots with ten consecutive runs per simulation.

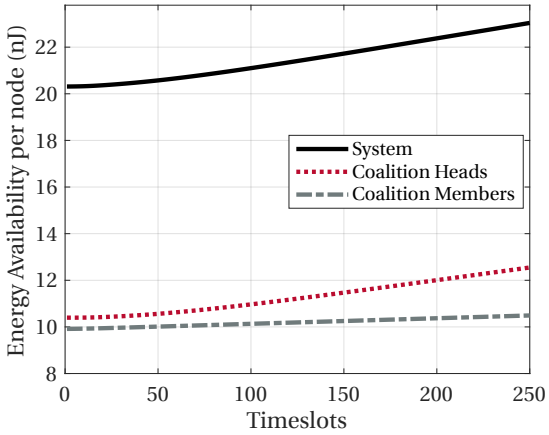
The framework's operation during a single UAV relocation period T is shown in Fig. 5.7 where statistical averages over 2000 different topologies (of $|M| = 51$ devices) are obtained and presented. As initial c_{th} value for each run we set $c_{th} = 10$, i.e. requiring 20% of nodes to act as coalition heads. Fig. 5.7a depicts the average consumed energy per node during a UAV relocation period of 250 timeslots. It is observed that the coalition head



(a) Consumed energy vs time



(b) Harvested energy vs time



(c) Energy availability vs time

Figure 5.7 Framework operation study during a UAV relocation period

energy consumption decreases due to the UAV mobility (towards the chs), while the same happens for the member nodes due to the learning process of the member-ch association. Similarly, Fig. 5.7b shows the average harvested energy per node suggesting that the critical emergency gateway coalition heads absorb increased energy levels as the UAV position converges and the eNB hovers above the nodes. Evidently, by examining Fig. 5.7a, and Fig. 5.7b the statistically averaged results reveal that the convergence time for the UAV

position is fairly small (e.g., 120-160 timeslots). Finally, the overall energy availability per node during the period T is shown in Fig. 5.7c. The energy availability curves combine the previous observations and verify that our solution, given an appropriate choice of P_{UAV} value, manages to provide increased support to the chosen coalition heads during the specific UAV relocation period.

5.8.3 Scalability, and Comparative Evaluation

In this subsection, we study the operation of our framework as a whole and provide comparative results against other alternatives. The various design options under evaluation, refer to the consideration of mobile versus stationary UAVs, and to the use of the MG methodology for selecting the devices' role, versus a purely random selection approach with respect to the role of a node (i.e., coalition head or member), still however maintaining the distributed nature of the overall process. For the case where a static UAV is assumed, we essentially consider a stationary UAV continuously hovering at the PS critical area's center at the h_{min} altitude. As a consequence, four different alternatives are evaluated, as follows: a) Use of both MG proposed approach and adaptive UAV positioning, as introduced in this chapter (denoted in the following as simply Mobile UAV), b) Use of only the MG proposed approach and assuming static UAV, (denoted in the following simply as Static UAV), c) Use of probabilistic random role selection process (i.e., no MG approach), while adaptive UAV positioning still applies, (denoted in the following as Mobile UAV - No MG), and d) Use of probabilistic random role selection process (i.e. no MG approach) and static UAV (denoted in the following as Static UAV - No MG). For all the following results we consider a UAV relocation period $T = 250$ timeslots, with ten consecutive runs per simulation. It is also noted that for all considered options, the power management optimization process as described in Section 4.2, as well as the coalition formation process detailed in Section 6, still apply for fairness purposes in the comparison.

By considering the aforementioned alternatives, we essentially evaluate both the impact of the UAV optimal positioning element of our approach on the overall PSN operation, as well as the role of the minority game whose operation maximizes the set of satisfied agents (the minority - here the chs) and bounds to their population ($\leq c_{th}$ - see Section 5.5). Specifically, Fig. 5.8 shows initially how the size of the IoT-inspired PSN impacts the

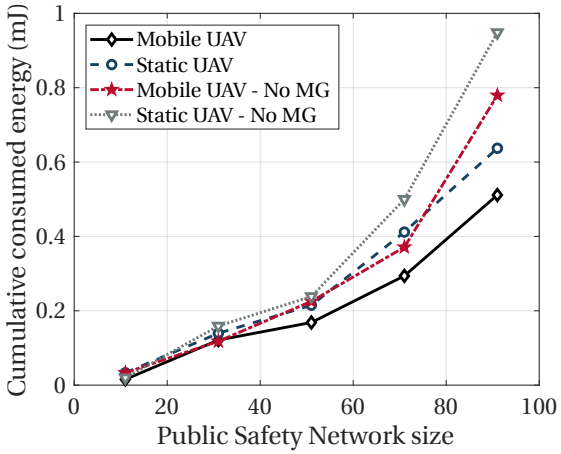


Figure 5.8 Cumulative consumed energy vs PSN size

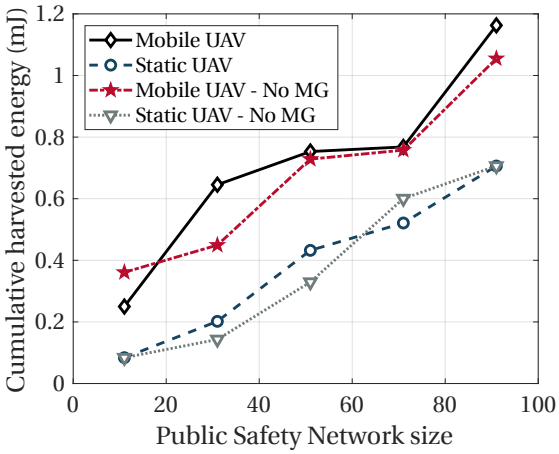


Figure 5.9 Cumulative harvested energy vs PSN size

consumed energy under all considered design alternatives. For topologies ranging from 11 to 91 IoT nodes, we present the cumulative energy consumption at the end of the 10^{th} relocation period. Similarly, Fig. 5.9 shows for the same topologies the cumulative harvested energy of the PSN at the end of the 10^{th} relocation period.

As the results of both Fig. 5.8 and Fig. 5.9 suggest the random ch (role) selection is presenting reduced performance due to the unpredictability of the ch population especially when a large number of IoT nodes is considered. In addition, since the random ch selection approach results in larger ch populations, the mobility of the UAV (even if when UAV adaptive positioning is performed) is limited leading to lower harvested energy levels (Fig. 5.8) along with increased transmission cost for the coalition heads and the IoT PSN as a whole (Fig. 5.9). Similar observations are drawn by analyzing the results in Fig. 5.8, where the static alternatives lead to a significant increase of the consumed uplink transmission power in the PSN when compared to their mobile counterparts. Accordingly, in Fig. 5.9 we also observe that our proposed framework leads to a system where the energy produced by the UAV is harvested more efficiently in comparison to all other alternatives. It should be noted that the overall framework's operation, as summarized in Section 5.2 and discussed in detail in Section 5.7, is of distributed nature requiring limited information exchange, and characterized by low computational complexity, as at each step the involved calculations

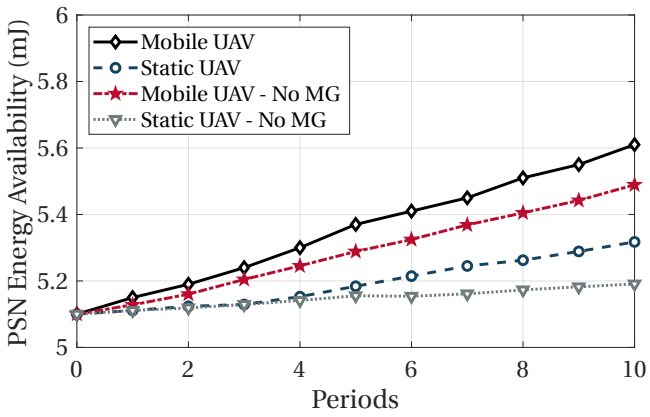


Figure 5.10 PSN energy availability vs time

are based on expressions of closed-form. Therefore, the overall complexity of the proposed framework is not affected as the number of IoT nodes increases.

Focusing further on the benefits obtained by the proposed framework, and in particular by the capability of UAV mobility, Fig. 5.10 presents the PSN's total energy availability vs. time which is expressed as consecutive relocation periods of 250 timeslots, for a scenario with $|M| = 51$ nodes. For these results, 100 different topologies were averaged for each considered option. As clearly seen in Fig. 5.10 the system energy availability under the mobile UAV/eNB proposed approach (for both Mobile UAV options) increases at a significantly higher rate, when compared with the cases of continuously stationary UAV (i.e. static UAV counterparts). This result reveals the positive impact that dynamic UAV-mounted eNB positioning has jointly on the energy harvesting efficiency and energy consumption reduction (both for WET and WIT phase). Evidently, the proposed solution assuming both UAV mobility and MG operation (i.e. mobile UAV) is superior to all other alternatives, resulting in a 2.3-time increase of the PSN's charging rate compared to the stationary UAV case (Static UAV options), and a 1.3-time increase compared to the random coalition head selection option (No MG options).

5.9 Related Work

The corresponding relevant work in this field can be broadly classified into three main categories as follows:

Communications Considerations

The inclusion of multi-sensor IoT devices to PSNs provides access to massive types of data (video from low-energy cameras, audio, IoT sensor environmental data, etc.) that can be crucial for situation awareness, post-emergency actions, and accident prevention. In addition, the heterogeneous nature of IoT devices [233] with the ability to communicate with different protocols and in a D2D manner offers low latency, increased PSN capacity, and in cases of infrastructure failures, manages to keep the PSN intact due to its decentralized nature. In the recent literature, a number of works investigate the impact of the IoT-based D2D communications and clustering techniques on PSNs. In [204], the use of LTE D2D communications is studied considering jointly homogeneous resources' interference along with interference from other RF-based systems. The results reveal that D2D-based PSN can achieve up to four times higher system throughput in realistic implementations in comparison to regular LTE settings. Finally, in [10], the authors propose a D2D communication architecture for PSNs that studies two scenarios of partially and totally damaged base stations, and selects UEs to operate as mobile relays that can reestablish the information flow, increase the system's capacity and extend the coverage area.

UAV-enabled Approaches

In order to further improve the PSN adaptivity considering the challenging conditions and enhance the IoT devices' energy sustainability, another line of research considers the use of unmanned aerial vehicles (UAVs) acting as base stations (BSs) [22, 308]. Due to their controllable mobility, the UAVs can approach and target specific ground PS-IoT devices and provide fast deployment, coverage extension, or reestablishment (after network failures), while maintaining reduced transmit power requirements for the IoT nodes [256]. In [200], the authors discuss the optimal location of a UAV when D2D underlaid links

are present, while in [201], the positioning of multiple UAVs in an IoT environment is investigated to provide efficient data aggregation. In [207], the authors present UAV-assisted communication attributes focusing on a drone cooperation scenario with conventional base stations. In [22], a game-theoretic mechanism is presented for load balancing between WiFi access points and LTE-Unlicensed base stations mounted on a UAV, utilizing a no-regret learning distributed scheme. Many key industry vendors have worked on projects of deploying airborne BSs for wireless connectivity, including Facebook's Project Aquila and Google's Project Loon (deployed in a disaster response scenario in Puerto Rico [323]). Finally, several research efforts have been devoted to the security aspects relevant to the operation of UAV-assisted solutions, and in particular to the problem of detecting malicious nodes in UAV-assisted networks in order to ensure reliable overall system operation [28, 159].

Wireless Powered Communication Integration

Finally, in recent literature, the flexible mobility of UAVs is coupled with the Radio Frequency (RF) wireless powered communication technique (WPC) [33] which has emerged as a promising solution for reliably supplying with energy the public safety environment nodes. The conventional WPC technique involves a static access point (AP) that is responsible for charging a set of wireless nodes in the downlink, while the nodes use the harvested energy by the RF signals to transmit their data back to the AP in the uplink. Two variations of WPC networks include the harvest-then-transmit model [220, 327] where -usually battery-less- devices utilize all or part of the harvested energy to transmit and the harvest-transmit-store model [317], where the devices are able to store energy leftovers for future exploitation. The proposed combination of a UAV-based AP aims to resolve the "doubly near-far" problem that usually appears in WPC networks where remote nodes receive reduced amounts of energy due to the RF propagation losses and at the same time need to use, higher transmission power in the uplink to transmit their information [327]. Thus in [220, 317, 327] a UAV is utilized to centrally charge a set of users (harvest-then-transmit WPC technique) and collect uplink information transmissions from the nodes.

The work in [327] proposes a mechanism to maximize the uplink throughput of a TDMA-based system over a certain UAV flight period and certain UAV speed constraints.

The proposed solution provides a set of hovering locations for the UAV and a trajectory of successive hover positions for a suboptimal solution to the uplink (information) and downlink (energy) power management problem with speed constraints. In [220], the authors investigate a TDMA-based WPC network, where the nodes utilize the harvest-then-transmit technique to harvest energy from a UAV-mounted base station. The aim is to maximize the system's minimum throughput performance by jointly considering the UAV trajectory, uplink power, and time resources. In [317], the authors propose a mechanism to maximize the throughput of the D2D wireless node with a static UAV deployed at varying altitudes acting as a WPC energy source under the harvest-transmit-store technique.

Finally, in [330], the authors also consider machine-to-machine (M2M) energy transfer with gateways charging the network's IoT devices in the downlink while transmitting information to a base station in the uplink. The aim is to minimize the overall energy consumption and the authors deploy a resource allocation mechanism (power control and time allocation) considering both non-orthogonal multiple access (NOMA) and time division multiple access (TDMA) strategies.

5.10 Conclusion

Our proposed approach exploits new capabilities offered by modern UAV-enabled data aggregators, and D2D wireless powered communication techniques while promoting decentralized IoT-node decision making. We present a coalition formation mechanism that enables IoT devices to autonomously choose roles and the respective receiver to be associated with (emergency gateway coalition head) within the PSN. This is achieved through a distributed Minority Game model, combined with reinforcement learning algorithms. D2D communication capabilities are utilized for information transmission towards a mobile UAV-assisted eNB, while a WPC-based mechanism enables IoT nodes to harvest energy from the UAV and subsequently transmit their data. The optimal position of the mobile UAV is determined by maximizing the coalition head energy availability. In addition, to further improve the overall system energy efficiency, a utility-based NOMA transmission power allocation approach is introduced, by formulating a power control problem and treating it as a non-cooperative, distributed game among IoT nodes. The outcome of the

game concludes with a unique Nash equilibrium that determines the nodes' optimal uplink transmission powers.

The operation and performance of our proposed framework were extensively evaluated through modeling and simulation, while the presented detailed numerical results demonstrate its superior energy efficiency, achieved by capitalizing on individual decision making and learning approaches, factors that are of paramount importance in IoT-based PSNs. Our current and future work contains the testing of the proposed framework in a realistic testbed environment for PS and disaster relief IoT applications.

Chapter 6

The Smart City Defense Game

The work in this chapter has been partially supported by the US National Science Foundation under the EPSCoR cooperative agreement Grant OIA-1757207. An extended version of this chapter is currently under review.

6.1 Introduction

Until now, we have focused on the Smart City's IoT infrastructure and specifically its use for passive crowd monitoring, and critical communication establishment and longevity. In this chapter, we shift our attention to city resource management during black swan events, and specifically during organized terrorist or insurrection threats in the context of a Smart City (SC) that relies on diverse technologies (e.g. Internet of Things (IoT), cloud computing, big data analytics, and artificial intelligence) [85, 160, 206]. Arguably, the intelligence of such SC environments also stems from their ability to make decisions related to the use and management of their natural and municipal resources, both in the short term and when accounting for future development [226]. This is not an easy task, especially since the SC organization incorporates a set of primal city entities with specific resource budgets, separate governance structures, and unique operational goals. Such smart city entities primarily include traffic and public transport authorities, departments overlooking critical cyber-physical facilities (i.e., intelligent buildings [272], smart grid [262, 263], natural gas, or water infrastructures [93]), information and communication technology (ICT) administra-

tions, and public safety/emergency service agencies (ESAs) [85]. Since these entities often operate on different conceptual levels (physical, cyber, social) within the city structure, the SC paradigm requires a management platform for supervision, coordination and optimal strategic allocation of SC resources, especially in cases of public safety threatening events such as adversarial/human-caused attacks [55, 177]. A case in point is Rio de Janeiro's SC operation center that integrates multiple individual agencies towards optimal disaster response and emergency management [278].

In response, high-level city adversaries on the physical plane like traditional terrorist organizations have advanced their tactics towards conflicting the maximum possible damage by distributing their forces across multiple city targets. The latest terrorist efforts attest to this observation with the Paris attacks in 2015 taking place simultaneously across six distinct physical locations [138], and the Brussels bombings in 2016 occurring in coordination across two different city targets [296]. Thus, terrorist strategies can be guided by knowledge related to the city authorities' structure such as the distribution of first response resources. This knowledge can be acquired by practical means including adversarial insiders, social engineering against city officers/employees (e.g., by social-media data exploitation), and long-term extraction/analysis of SC open data.

In addition, amidst the era of social media (SM), terrorist groups are rapidly exploiting technological advancements and trends to improve their tactics [41]. This adaptation creates new city vulnerabilities for exploitation, especially since social media are considered a cyber-social extension of the future SC. Interestingly, in the last decade, the increasing adaptation of SM by citizens and ICT city agencies during emergencies creates a propagation of information to many directions [241]. This includes citizen to citizen (self-organization, alerting and aid), SC ICT agencies to citizens (and traditional media to citizens - for public alerting and guidance), and citizens to ICT agencies (SM integration into monitoring environments for intelligence extraction, situation awareness, and immediate response) [143, 241, 296, 329]. Examples of the massive use of SM during terrorist attacks include the Brussels bombings in 2016 [296], and the Boston Marathon bombings in 2013 [290, 338], where a major concern regarding the credibility of posted information emerged. Specifically, during this incident, the diffusion of misinformation and speculation through Twitter actively endangered individual lives and lead to misuse of emergency response resources [290, 338]. This emerging dependency on SM during crises can be exploited by sophisticated SC

adversaries to produce misinformation streams towards directing the public to unsafe city zones or actively obstructing the operation of an SC ESAs (see [145], and [13]). To this end, next-generation terrorist organizations can make use of massive social bots [318] to generate targeted SM posts, or partner with hacker communities to infiltrate SC alerting/ICT infrastructures [247].

We consider a multi-layer smart city model and present a defense mechanism for optimal SC resource allocation in response to simultaneous terrorist attacks of various types [89, 242]. The key contributions of this chapter are summarized as follows:

- A Smart City is modeled as a multi-dimensional setting which consists of a lower physical plane and an upper cyber-social one. The physical layer is a set of distinct SC physical locations and city points of interest, while the social layer consists of multiple cyber spaces that include social media, web pages and chat spaces.

- By considering a Terrorist Organization (TO) attack taking place in both SC layers, we model the optimal response of two SC agencies responsible for public safety and SC defense, namely an Emergency Service Agency (ESA) operating at the physical layer and an Information and Communication Technology (ICT) agency operating at the Cyber-Social SC plane. Each organization aims to deploy its financial resources optimally across multiple spaces of interest either physical or cyber, by also considering the possibility of budget exchange with the other agency. We also take into account the TO financial strength and respective budget allocation across SC targets. In order to fully capture the inter-dependencies and interactions among all the conflicting parties we introduce a multi-stage Smart City Defense Game (SCDG) with observed actions and compute the game's subgame perfect Nash equilibrium that describes the optimal strategies of all players focusing on the optimal budget exchange among the SC agencies that minimizes the expected number of successful TO attacks across the two SC layers and targets.

- Detailed numerical and comparative results demonstrate that the proposed Smart City Defense Game is a promising solution for modeling SC agencies' resource allocations, internal budget transfers and interactions with a conflicting party towards securing the cyber-physical Smart City of the future.

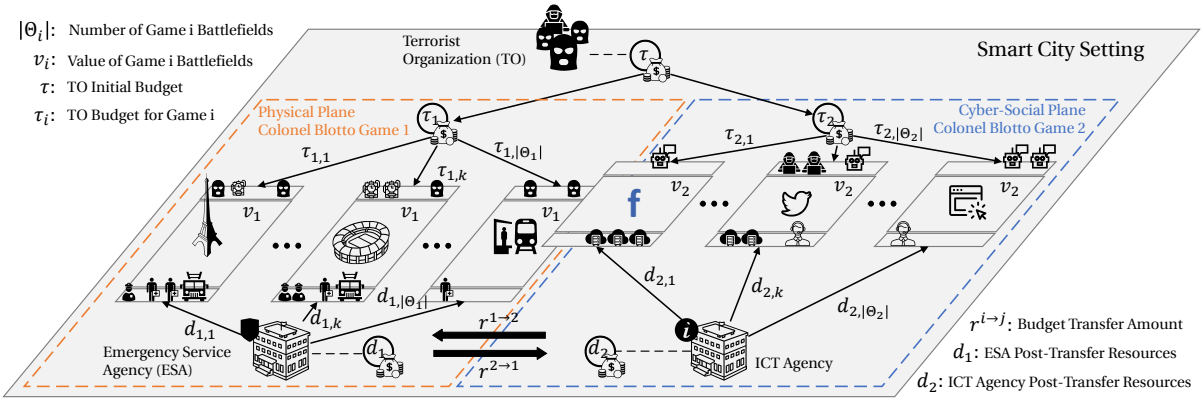


Figure 6.1 Smart City Defense Game: Players, Games, and Components

6.2 Game Model and Problem Formulation

In this section we set the stage for the proposed Smart City security game which is formulated as a complete information multi-stage game with three players.

6.2.1 Attack and Defense Scenarios

Consider a smart city adversary, namely a Terrorist Organization (TO) T with finite available resources represented by a financial budget τ. The organization deploys a parallel attack towards the SC targeting simultaneously two separate conceptual levels. At the first level, the TO uses a part of its financial resources, denoted as τ_1 to perform physical attacks on multiple critical SC area targets by allocating attack budget to each site that can be translated to human agents (suicide vehicles, bombers, shooters, etc.) or attacking equipment. In response, the SC's emergency service agency (ESA) deploys its own financial resources denoted as c_1 across the critical targeted areas for defense and disaster prevention purposes [89]. The ESA's budget can be translated to first responder units (human resources, police, firefighters, medical personnel) and emergency management equipment.

In addition, in our model, the sophisticated terrorists attack concurrently a second "cyber-social" level of the SC environment by using another part of their resource budget τ_2 with $\tau_1+\tau_2=\tau$. This is achieved by allocating the τ_2 attack budget to disseminate misinformation across multiple social media, traditional media sites or SC alerting infrastructure

towards either obscure the truth to affect the general public or temper with social sensing applications utilized by the SC entities [143, 296, 329, 338]. The cyber-social attack budget is utilized by the adversary either towards securing computational resources to enable autonomous social-bot operation for misinformation diffusion [98, 318] or for acquiring human resources responsible for the same task (partner with hacker organizations under hire, etc. [247]). On the SC defense side, the ICT administration which is responsible for securing the information-related SC layers utilizes its pre-allocated defense budget c_2 by allocating it across the different social media entities under attack. The ICT financial resources can be used either

1. for deploying ICT administration human resources responsible for identifying/exposing unreliable sources and providing trustworthy news to the public, or

2. for dynamically securing and acquiring cloud computing resources (usually offered by public cloud service providers [271], similar to the case of IBM in Rio [278]). Such resources (computing power for real-time data analytics and machine learning frameworks [271]) can be utilized for deploying truth discovery algorithms that identify misinformation in the presence of noisy data from unvetted SM sources (e.g., as in [338] where the proposed solution was evaluated against real-world Twitter datasets extracted from recent terrorist attacks). An interesting empirical study on fighting terrorism on social media is presented in [242]. A survey on anti-terrorism technologies for social media is presented in [13].

For both scenarios, we will assume that the party that has allocated the majority of resources in each targeted area (either physical or cyber-social) has successfully achieved his goal (landed a successful attack or managed to defend the target). Since the satisfaction of each player depends not only on his actions but also on the actions of his opponent (i.e., the number of resources strategically allocated) we can use game theory to model their interactions [106]. Thus, in order to model (a) the player interactions on the two parallel city levels (physical and cyber-social) and (b) model their allocation of budget across multiple city area targets and across multiple cyber-social spaces (e.g. different social media), we assume that the TO participates concurrently to two Colonel Blotto games [243] against the two city entities. We will further assume that the two SC entities are able to form a coalition

towards exchanging emergency resources if it is beneficial for both of them. In order to model this resource transfer and examine its characteristics given the TO's own allocation of resources among his two rivals (i.e., the two SC entities and in extension the two SC layers) we formulate a multi-stage complete information Smart City Defense Game (SCDG) which is partly based on the multi-stage Blotto game described in [165]. In what follows we define and describe the basic parts of the game.

6.2.2 The Colonel Blotto Game

The continuous colonel Blotto Game [243] models the strategic resource allocation between two opponents with finite infinitely divisible resources (troops) in a competitive environment that consists of multiple battlefields. The two opponents play the game by allocating their troops to each battlefield. The player that allocated the larger amount wins the battlefield while their objective is to win as many battles as possible. It is an one-shot game defined as CBG$\{P, \{F^p\}_{p\in P}, \{S^p\}_{p\in P}, \Theta, v, \{U^p\}_{p\in P}\}$ where:

- $P \triangleq \{P_A, P_B\}$ denotes the two opponents/players
- F^p are the available resources of player $p \in P$
- S^P is the set of strategies for player p, $p \in P$
- Θ is the set of the game's battlefields with $\theta = |\Theta|$
- v denotes the value of each battlefield
- U^p is the utility function of player p, $p \in P$

The two players distribute their total forces F^p across the n battlefields with the allocation vector of player p being $\boldsymbol{f}^p = [f_1^p, ..., f_k^p, ..., f_n^p]$, where f_k^p is the resource amount assigned to battlefield k. Thus, the strategies of each player is the set S^p of all the possible allocations across the battlefield:

$$S^p \triangleq \{\boldsymbol{f}^p \mid \sum_{k=1}^{\theta} f_k^p \leq F^p, \;\; f_k^p \geq 0\}$$

Each battlefield is won by the player with the highest resource contribution, while the payoff of player p from winning a single battlefield k is defined as:

$$u_k^p(f_k^p, f_k^{-p}) = \begin{cases} v & \text{if } f_k^p > f_k^{-p} \\ 0 & \text{if } f_k^p < f_k^{-p} \\ \frac{v}{2} & \text{if } f_k^p = f_k^{-p} \end{cases}$$

where f_k^{-p} denotes the opponent's resource contribution to battlefield k. The opponent's payoff per battlefield is $u_k^{-p}(f_k^p, f_k^{-p}) = v - u_k^p(f_k^p, f_k^{-p})$. The overall utility of each player is defined as:

$$U^p(\boldsymbol{f}^p, \boldsymbol{f}^{-p}) = \sum_{k=1}^{\theta} u_k^p(f_k^p, f_k^{-p})$$

The goal of each player p is to choose a strategy in S^p (i.e., a resource allocation vector) that maximizes his utility and number of won battlefields given his opponent's selected strategy.

Definition 2. *For the CBG a strategy profile* $\{\boldsymbol{f}^{p*}, \boldsymbol{f}^{-p*}\}$, $\boldsymbol{f}^{p*} \in S^p$ *and* $\boldsymbol{f}^{-p*} \in S^{-p}$ *is a pure-strategy Nash equilibrium if for player* p*:*

$$U^p(\boldsymbol{f}^{p*}, \boldsymbol{f}^{-p*}) \geq U^p(\boldsymbol{f}^p, \boldsymbol{f}^{-p*}),\ \forall \boldsymbol{f}^p \in S^p. \tag{6.1}$$

It has been proven in [243] that the CBG is not guaranteed to yield a NE in pure-strategies. Therefore, a NE for the CBG exists in mixed-strategies, where each opponent $p \in P$ chooses a multi-variant probability density function over S^p (assigns a probability for playing each pure strategy). A CBG mixed strategy for player p is a distribution of resources expressed by a θ-variate distribution function $O^p : \mathbb{R}_+^\theta \longrightarrow [0,1]$ with support contained inside the set S^p of feasible resource allocations.

Definition 3. *Let* $\mathcal{Q}^{p*}$ *be the set of all probability distributions over player's* p *pure-strategy space* S^p*. For the CBG a mixed strategy profile set* $\{O^{p*}, O^{-p*}\}$ *is a mixed-strategy Nash equilibrium (MSNE) if for player* p*:*

$$U^p(O^{p*}, O^{-p*}) \geq U^p(O^p, O^{-p*}),\ \forall O^p \in \mathcal{Q}^p. \tag{6.2}$$

Each θ-variate distribution function O^p is associated with a set of univariate marginal

distribution functions $\{\Phi_k^p\}_{k=1}^{\theta} : \mathbb{R}_+ \longrightarrow [0,1]$ for each battlefield k. For a player p, given his mixed strategy NE, the forces' allocation vector $\boldsymbol{f}^p = [f_1^p, ..., f_k^p, ..., f_n^p]$ is drawn from O^p with f_k^p being a random variable drown from Φ_k^p.

6.2.3 The Smart City Defense Game (SCDG)

Given the SC attack/defense scenarios and the CBG discussion above we formulate a multi-stage SC Defense Game (SCDG) with observed actions that consists of three players and captures all interactions between allies and opponents. The two SC entities, namely the Emergency Service Agency and the ICT agency, that will be denoted as player 1 and 2 respectively, fight against the Terrorist Organization denoted by T. The pre-allocated financial defense budget of each SC player $i \in \{1,2\}$ is c_i, while the Terrorist organization's attack budget is τ. The two-layer conflict takes place simultaneously across θ_1 SC area physical targets (set Θ_1) that yield a payoff of v_1 to the winner (TO or ESA agency), and across θ_2 social media/cyber-social targets (set Θ_2) that yield a payoff of v_2 to the winner (TO or ICT agency) assuming $\theta_i \geq 3 \; \forall i \in \{1,2\}$ and $b_i, v_i \in \mathbb{R}$.

The SCDG is an extensive form perfect information game whose model parameters and actions taken by all players during previous stages are common knowledge. Thus, at the beginning of each stage there is a well-defined history h_{stage}, and a set of all possible histories H_{stage}. For this initial first stage $h_1 = \emptyset$, and $\Pi = \{c_1, c_2, \tau, v_1, v_2, \theta_1, \theta_2\}$ is the set of initial SCDG parameters that describe the setting. During the first stage the two SC entities form a coalition and choose whether to make a budget transfer towards their ally or not while the TO performs no action. We denote the amount of financial resource transfer from SC agency i to agency j as $r^{i\to j} \in [0, c_i]$, while $\{r^{1\to 2}, r^{2\to 1}\}$ is a first stage action profile. Each SC entity's i transfer amount (its first stage strategy) is given by the the function $R^i : \Pi \to A_1^i(\Pi)$, where as A_1^i we denote the set of all available first stage transfer actions of SC agency i. Following the budget transfer, the SC agency's i defense endowment is given by:

$$d_i(r^{i\to j}, r^{j\to i}) = c_i - r^{i\to j} + r^{j\to i} \;\; \forall i, j \in \{1,2\}, \; i \neq j \tag{6.3}$$

The SC entities' budget transfer is observed by the adversary T who, at the second stage of the game, decides on his resource allocation across the two battles/games (physical and cyber-social) and against the two SC defense opponents that perform no action in

this stage. The action history after stage one is $h_2 = \{r^{1\to2}, r^{2\to1}\}$, and H_2 is the set of all possible histories (SC alliance budget exchanges). Given h_2 the TO allocated budget τ_1 to fight the physical SC battle and budget τ_2 to fight at the cyber-social layer with $\tau_1 + \tau_2 \leq \tau$. Thus, the stage two action profile is $\{\tau_1, \tau_2\}$ with $A_2^T(H_2)$ being the set of all available budget τ divisions across the two SC layers. The TO's strategy during this stage is expressed by the amount he chose to allocate to the physical attack effort and is given by a function $\mathscr{T} : H_2 \to A_2^T(H_2)$, i.e., $\tau_1 = \mathscr{T}(h_2) = \mathscr{T}(r^{1\to2}, r^{2\to1})$. It follows that $\tau_2 = \tau - \tau_1$.

Entering the final stage of the SCDG the history is formed as $h_3 = \{h_1, h_2\} = \{r^{1\to2}, r^{2\to1}, \tau_1, \tau_2\}$ with H_3 being the set of all possible histories up to this point. During this SCDG stage the adversary TO participates in parallel to two CBGs (physical and cyber-social) that model his interactions with the SC defenders across all targets. Thus for each front i and against a SC entity i we formulate two CBGs $\forall i \in \{1,2\}$, namely:

$$CBG_i\{\{T,i\},\{\tau_i, d_i\},\{S_i^T, S^i\},\Theta_i, v_i,\{U_i^T, U^i\}\} \tag{6.4}$$

with budget allocation vectors across physical and cyber-social battlefields k denoted as $\boldsymbol{t}_i = [\tau_{i,1}, ..., \tau_{i,k}, ..., \tau_{i,\theta_i}]$, and $\boldsymbol{d}_i = [d_{i,1}, ..., d_{i,k}, ..., d_{i,\theta_i}]$ for the TO T and SC entities i, $i \in \{1,2\}$ respectively with $\sum_{k=1}^{\theta_i} \tau_{i,k} \leq \tau_i$, $\tau_{i,k} \geq 0$, and $\sum_{k=1}^{\theta_i} d_{i,k} \leq d_i$, $d_{i,k} \geq 0$. As discussed in subsection 6.2.2 these two games yield mixed strategy NEs where the players' budget allocation vectors across battlefields as seen in subsection 6.2.2 consist of random variables $\tau_{i,k}, d_{i,k}$ characterized by the univariant distribution functions $\{\mathfrak{T}_{i,k}\}_{k=1}^{\theta_i}$ and $\{\mathfrak{D}_{i,k}\}_{k=1}^{\theta_i}$, $\forall i \in \{1,2\}$ respectively for each SC target $k \in \Theta_i$.

The mixed strategies (the θ_i-variate distribution functions as defined in subsection 6.2.2) that express the distribution of budget for each player across the two CBGs' battlefields are:

$$O^1(h_3) = O^1(r^{1\to2}, r^{2\to1}, \tau_1, \tau_2),\ O^2(h_3) = O^1(r^{1\to2}, r^{2\to1}, \tau_1, \tau_2)$$
$$O_1^T(h_3) = O_1^T(r^{1\to2}, r^{2\to1}, \tau_1, \tau_2),\ O_2^T(h_3) = O_2^T(r^{1\to2}, r^{2\to1}, \tau_1, \tau_2)$$

The MSNEs characterize a state for the two games where the two SC defenders have chosen their optimal randomization over their budget allocation across battlefields (SC area targets for game 1, cyber-social spaces for game 2) and thus they cannot improve the SC protection by making a different choice. In addition, the MSNEs for the TO across the

two CBGs he participates in, are two probability distributions that capture his τ_1, τ_2 budget allocations over battlefields towards maximizing his expected utility, namely the number of physical areas and social-media environments he will successfully strike. For the proposed SCDG the use of mixed strategies for both fronts/games is motivated by the fact that both the TO and the SC entities have to randomize over their strategies towards preventing their opponent to guess their potential action.

Let us now define the overall strategy profile of each SCDG player, which is a collection of maps from all possible histories into available actions, namely:

$$\begin{aligned} \zeta^i &\triangleq \{R^i, O^i\} \ \ \forall i \in \{1,2\} \\ \zeta^T &\triangleq \{\mathscr{T}, O_1^T, O_2^T\} \end{aligned} \tag{6.5}$$

where ζ^i are the strategies (collection of functions) of the city entity i, $i \in \{1,2\}$, and ζ^T denotes the TO's strategies. Thus, the strategy profile is $\zeta = \{\zeta^1, \zeta^2, \zeta^T\}$ and the set that contain all possible player strategies is denoted as $Z \triangleq \{Z^1, Z^2, Z^T\}$, where $Z^p,\ p \in \{1,2,T\}$ is the set containing all possible actions of SCDG player p.

Given the allocation of budget of the three players to each battlefields of the two parallel CBGs (final stage), we will further define the SCDG's terminal history as $h_{terminal} = \{r^{1\to 2}, r^{2\to 1}, \tau_1, \tau_2, \boldsymbol{t}_1, \boldsymbol{t}_2, \boldsymbol{d}_1, \boldsymbol{d}_2\}$ and as $H_{terminal}$ the set of all possible terminal histories. Finally, as $\mathscr{H} = H_1 \cup H_2 \cup H_3 \cup H_{terminal}$ we denote the set of possible histories. Given the mixed strategies of each player, and the CBG definition in subsection 6.2.2 the SCDG payoff functions following the final stage are $\Psi^i : H_{terminal} \to \mathbb{R}, \forall i \in \{1,2\}$, and $\Psi^T : H_{terminal} \to \mathbb{R}$. Since the strategy profile ζ^p of each player p, $p \in \{1,2,T\}$ determines the SCDG's action path (i.e the $H_{terminal}$) we can express the payoffs as:

$$\begin{aligned} \Psi^i(\zeta^1, \zeta^2, \zeta^T) &\triangleq \mathbb{E}\Bigg[\sum_{k=1}^{\theta_i} u_k^i(\tau_{i,k}, d_{i,k})\Bigg] \triangleq E\Big[U^i\Big] \\ \Psi^T(\zeta^1, \zeta^2, \zeta^T) &\triangleq \mathbb{E}\Bigg[\sum_{i=1}^{2}\sum_{k=1}^{\theta_i} u_{i,k}^T(\tau_{i,k}, d_{i,k})\Bigg] \triangleq E\Big[U_1^T + U_2^T\Big] \end{aligned} \tag{6.6}$$

where:

$$u_k^i(\tau_{i,k}, d_{i,k}) = \begin{cases} v_i & \text{if } d_{i,k} > \tau_{i,k} \\ 0 & \text{if } d_{i,k} < \tau_{i,k} \\ \frac{v_i}{2} & \text{if } d_{i,k} = \tau_{i,k} \end{cases} \quad \forall i \in \{1,2\}$$

$$u_{i,k}^T(\tau_{i,k}, d_{i,k}) = v_i - u_k^i(\tau_{i,k}, d_{i,k})$$

with $d_{i,k}, \tau_{i,k}$ being the random variables that denote the budget allocated by the players to a battlefield k. The formal definition of the finite complete information SCDG is:

$$SCDG\Big\{\{1,2,T\},\{\mathscr{H}\},\{Z\},\{R_1,R_2,\mathscr{T},O^1,O^2,O_1^T,O_2^T\},\{\Psi^1,\Psi^2,\Psi^T\}\Big\}.$$

Definition 4. *A behavior strategy profile $\zeta^* \triangleq \{\zeta^{1*},\zeta^{2*},\zeta^{T*}\}$ in the strategy set $Z \triangleq \{Z^1,Z^2,Z^T\}$ is a Nash equilibrium of the SCDG with set of players $P \triangleq \{1,2,T\}$ if*

$$\Psi^p(\zeta^{1*},\zeta^{2*},\zeta^{T*}) \geq \Psi^p(\zeta^p,\zeta^{-\mathbf{p}*}),\ \forall \zeta^p \in Z^p,\ p \in P. \tag{6.7}$$

6.3 Subgame Perfect Nash Equilibrium of the SCDG

Since the SCDG is a multi-stage complete information game in extensive form we define a subgame perfect Nash equilibrium that requires the strategy of each player to be optimal after every stage history and not just at the beginning of the game [106].

Definition 5. *Given a stage ϵ history h_ϵ, $G(h_\epsilon)$ is a SCDG's subgame happening after h_ϵ and $\zeta^p|h_\epsilon$ is the restriction of player's p, $p \in \{1,2,T\}$ strategies to histories in $G(h_\epsilon)$. Then a behavior strategy profile ζ is a subgame perfect Nash equilibrium if for every h_ϵ, the restriction $\zeta|h_\epsilon$ is a Nash equilibrium in $G(h_\epsilon)$.*

For such multi-stage games with observed actions we can verify that a strategy profile ζ is subgame perfect by ensuring that no player p can increase his utility by deviating from ζ in a single stage and reverting to ζ for the rest of the game. This is verified by using the one-stage deviation principle for finite games.

Theorem 3. *The SCDG strategy profile ζ^* is a subgame perfect Nash equilibrium (SPNE) if and only if it satisfies the one-stage-deviation condition that for all players p, $p \in \{1,2,T\}$, stages ϵ, and histories h_ϵ:*

$$\begin{aligned} &\Psi^p(\zeta^{p*}, \zeta^{-\mathbf{p}*}|h_\epsilon) \geq \Psi^p(\zeta^p, \zeta^{-\mathbf{p}*}|h_\epsilon) \\ &s.t.\ \ \zeta^p(h^\epsilon) \neq \zeta^{p*}(h_\epsilon) \\ &\zeta^p_{|h_\epsilon}(h_{\epsilon+\omega}) = \zeta^{p*}_{|h_\epsilon}(h_{\epsilon+\omega}) \\ &\forall \omega > 0,\ \forall \zeta^p \in Z^p,\ \forall p \in \{1,2,T\}. \end{aligned} \tag{6.8}$$

Proof. The proof of Theorem 3 can be found in [106]. □

In order to derive the SPNE, for the SCDG we will apply backward induction since the game is of perfect information with exactly three stages (a finite number) [106]. The process identifies the equilibria in the latest stages and moves up until the initial stage of the extensive form game. In our case the backward induction algorithm initially considers the payoffs obtained by the optimal choice of the three players in the final Colonel Blotto games stage (Nash Equilibrium) that maximizes their payoff. In what follows, we describe the backward induction process towards determining their SCDG SPNE, focusing on the budget allocation strategies of the TO, ESA, and ICT agency.

6.3.1 Colonel Blotto Nash Equilibrium Payoffs

First, we focus our attention to the payoffs of the three players at the Nash Equilibrium of the two CBGs that take place at the physical (CBG_1) and the cyber-social plane (CBG_2) of the smart city. Given the definition in Section 6.2.2 and the analysis of the static CBG in [243] the payoffs for each player depend on the initial budgets τ_i (for the TO), d_i (for each SC entity), and are given as follows.

For each static CBG_i of value $\phi_i = |\Theta_i| \cdot v_i$ that takes place at the third stage of the SCDG there exist a Nash equilibrium with unique payoff for a SC entity player i, $i \in \{1,2\}$ playing

against the TO T, $i \in \{1,2\}$. Each SC player's payoff is [127]:

$$U^i(\tau_i, d_i) = \begin{cases} 0, & if \ \frac{d_i}{\tau_i} < \frac{1}{|\Theta_i|} \\ \phi_i\left(\frac{2\cdot\beta-2}{\beta\cdot|\Theta_i|^2}\right), & if \ \frac{1}{|\Theta_i|} \leq \frac{d_i}{\tau_i} < \frac{1}{|\Theta_i|-1} \\ \phi_i\left(\frac{2}{|\Theta_i|} - \frac{2\cdot\tau_i}{|\Theta_i|^2\cdot d_i}\right), & if \ \frac{1}{|\Theta_i|-1} \leq \frac{d_i}{\tau_i} < \frac{2}{|\Theta_i|} \\ \phi_i \cdot \frac{d_i}{2\cdot\tau_i}, & if \ \frac{2}{|\Theta_i|} \leq \frac{d_i}{\tau_i} < 1 \\ \phi_i - \phi_i \cdot \frac{\tau_i}{2\cdot d_i}, & if \ 1 \leq \frac{d_i}{\tau_i} < \frac{2}{|\Theta_i|} \\ \phi_i - \phi i\left(\frac{2}{|\Theta_i|} - \frac{2\cdot d_i}{|\Theta_i|^2\cdot\tau_i}\right), & if \ \frac{2}{|\Theta_i|} \leq \frac{d_i}{\tau_i} < |\Theta_i|-1 \\ \phi_i - \phi_i\left(\frac{2\cdot\beta'-2}{\beta'\cdot|\Theta_i|^2}\right), & if \ |\Theta_i|-1 \leq \frac{d_i}{\tau_i} \leq |\Theta_i| \\ \phi_i, & if \ |\Theta_i| < \frac{d_i}{\tau_i} \end{cases} \tag{6.9}$$

where $\beta = \left\lceil \frac{\frac{d_i}{\tau_i}}{1-(|\Theta_i-1)\frac{d_i}{\tau_i}} \right\rceil$, and $\beta' = \left\lceil \frac{\frac{\tau_i}{d_i}}{1-(|\Theta_i-1)\frac{\tau_i}{d_i}} \right\rceil$. Accordingly the payoff of the TO for the CBG_i, $i \in 1,2$ is:

$$U_i^T(\tau_i, d_i) = \phi_i - U^i(\tau_i, d_i) \tag{6.10}$$

where τ_i is the TO budget allocated for game i and d_i the SC entity's i, $i \in 1,2$ budget entering the SCDG final stage.

The authors in the seminal work [243] provide a proof of the existence of the equilibrium in the CBG. Determining the MSNE for the CBG and thus the θ-variate distributions is not trivial and an active research area [96, 244]. A number of approaches have been proposed including fictitious play [128], and geometric methods [303] while the latest research works rely on dynamic programming approaches to solve the discrete version of the game [31, 314]. Since it is out of the scope of this work we will omit MSNE construction details. Evidently, the final payoffs of the SC entities critically depend on the budget levels after the resource transfer which is the phenomenon we try to model in this work.

Given the definition of the SCDG payoffs for the three players as presented in Eq. 6.6, there are 64 unique forms of the SCDG payoff function Ψ^T for the SC adversary TO T (8 possible payoffs from CBG_1 and another 8 from CBG_2). This leads to a vast number of SPNE that complicate the tractability of our solution. Therefore, in order to simplify our analysis, we will assume that the number of battlefields for the two games is arbitrarily large, which is physically supported by the fact that the examined SC environment consists of a very large number of possible physical targets and even larger number if social environments in

the cyber space. In this case, the number of unique TO payoffs Ψ^T collapses to 4 and Eq. 6.9-6.10 can be rewritten as:

$$U^i(\tau_i, d_i) = \begin{cases} \phi_i \cdot \frac{d_i}{2 \cdot \tau_i},), & if \ \ \frac{2}{|\Theta_i|} \leq \frac{d_i}{\tau_i} < 1 \\ \phi_i - \phi_i \cdot \frac{\tau_i}{2 \cdot d_i}, & if \ \ 1 \leq \frac{d_i}{\tau_i} < \frac{2}{|\Theta_i|} \end{cases} \tag{6.11}$$

$$U_i^T(\tau_i, d_i) = \phi_i - U^i(\tau_i, d_i)$$

6.3.2 Smart City Defense Game Families of Equilibria

Given the NE payoffs in the game's third stage, we compute the SPNE for the SCDG for each player during the second and first SCDG stage. In what follows, we define the total budget transfer from the ESA (SC entity 1) to the ICT agency (SC entity 2) as r.

Theorem 4. *For the SCDG where $\phi_1 = |\Theta_1| \cdot v_1$ is the value of the physical CBG, $\phi_2 = |\Theta_2| \cdot v_2$ is the value of the cyber-social CBG and prior to the third game stage:*

- *the available budget of the ESA is $d_1 = c_1 - r$*
- *the available budget of the ICT agency is $d_2 = c_2 + r$*
- *the total available budget of the TO T is τ, and*
- *$\frac{2}{|\Theta_1|} < \frac{\tau}{d_1} < 1$ and $\frac{2}{|\Theta_2|} < \frac{\tau}{d_2} < 1$*

then the second SCDG stage equilibrium strategy for the TO that maximizes its payoff is:

$$\tau_1^* = T^*(r^{1 \to 2}, r^{2 \to 1}) = \begin{cases} any \ choice \in [0, \tau], & if \ \ \frac{\phi_1}{d_1} = \frac{\phi_2}{d_2} \\ \tau, & if \ \ \frac{\phi_1}{d_1} > \frac{\phi_2}{d_2} \\ 0, & if \ \ \frac{\phi_1}{d_1} < \frac{\phi_2}{d_2} \end{cases} \tag{6.12}$$

$$\tau_2^* = \tau - \tau_1^*$$

In this case if the SCDG parameters also satisfy either
$\frac{\phi_1}{c_1} < \frac{\phi_2}{c_2}$, $\frac{2}{|\Theta_1|} < \frac{\tau}{c_1 - \frac{\phi_2 c_1 - \phi_1 c_2}{\phi_1 + \phi_2}} < 1$ & $\frac{2}{|\Theta_2|} < \frac{\tau}{c_2 + \frac{\phi_2 c_1 - \phi_1 c_2}{\phi_1 + \phi_2}} < 1$
or

$\frac{\phi_1}{c_1} > \frac{\phi_2}{c_2}, \frac{2}{|\Theta_1|} < \frac{\tau}{c_1 - \frac{\phi_1 c_2 - \phi_2 c_1}{\phi_1 + \phi_2}} < 1$ & $\frac{2}{|\Theta_2|} < \frac{\tau}{c_2 + \frac{\phi_1 c_2 - \phi_2 c_1}{\phi_1 + \phi_2}} < 1$, *then the first SCDG stage equilibrium strategies for the two SC entities that maximize their payoff are:*

$$R^{*1} = r^{*1\to 2} = \begin{cases} \rho \in [0, \frac{\phi_2 c_1 - \phi_1 c_2}{\phi_1 + \phi_2}), & if \ \ \frac{\phi_1}{c_1} < \frac{\phi_2}{c_2} \\ 0, & otherwise \end{cases} \tag{6.13}$$

$$R^{*2} = r^{*2\to 1} = \begin{cases} \rho \in [0, \frac{\phi_1 c_2 - \phi_2 c_1}{\phi_1 + \phi_2}), & if \ \ \frac{\phi_1}{c_1} > \frac{\phi_2}{c_2} \\ 0, & otherwise \end{cases} \tag{6.14}$$

and there exists a SCDG SPNE family of $\{T^*, R^{*1}, R^{*2}\}$ *as defined above.*

Proof. see Appendix A.1. □

Theorem 4 completely characterizes the SPNE actions of all SCDG participants in the case where the TO has the smallest available budget among all conflicting parties, following the SC budget transfer. In such a case the TO chooses to allocate his entire initial budget to a single CBG taking into account this game's value along with the strength of his opponent budget-wise. If both players are equally unattractive for the TO he randomizes his budget allocation towards the two fights-CBGs. In response, according to the SPNE, the SC entity whose plane is not under threat will transfer budget to the other SC player within a set as his payoff will not be affected by this action. The transfer will take place even if the party that provides resources has less initial budget than his ally. The existence of the upper bound in this transfer guarantees the TO's action and essentially the SPNE's existence.

Theorem 5. *For the SCDG where* $\phi_1 = |\Theta_1| \cdot v_1$ *is the value of the physical CBG,* $\phi_2 = |\Theta_2| \cdot v_2$ *is the value of the cyber-social CBG and prior to the third game stage:*

- *the available budget of the ESA is* $d_1 = c_1 - r$
- *the available budget of the ICT agency is* $d_2 = c_2 + r$
- *the total available budget of the TO* T *is* τ*, and*
- $d_1 + d_2 < \tau$, $\frac{2}{|\Theta_1|} < \frac{\tau_1}{\frac{\tau}{1+\sigma}} < 1$ *and* $\frac{2}{|\Theta_2|} < \frac{\tau_2}{\frac{\sigma \cdot \tau}{1+\sigma}} < 1$

where $\sigma = \sqrt{\frac{\phi_2 d_2}{\phi_1 d_1}}$*, then the second SCDG stage equilibrium strategy for the TO that maximizes its payoff is:*

$$\begin{aligned} \tau_1^* = T^*(r^{1\to 2}, r^{2\to 1}) &= \frac{\tau}{1+\sqrt{\frac{\phi_2 d_2}{\phi_1 d_1}}} \\ \tau_2^* &= \tau - \tau_1^* \end{aligned} \tag{6.15}$$

In this case the first SCDG stage equilibrium strategies for the two SC entities that maximize their payoff are:

$$R^{*1} = r^{*1\to 2} = \begin{cases} \frac{c_1-c_2}{2} - \frac{c_1+c_2}{2} \cdot \sqrt{\frac{\phi_1}{\phi_1+\phi_2}}, & if \ \ \frac{c_1-c_2}{2c_1c_2} > \sqrt{\frac{\phi_1}{\phi_2}} \\ 0, & otherwise \end{cases} \tag{6.16}$$

$$R^{*2} = r^{*2\to 1} = 0$$

and there exists a SCDG SPNE family of $\{T^*, R^{*1}, R^{*2}\}$ *as defined above. For the case where the budget strength of the two SC allies is interchanged the same SPNE family exists with the reverse budget transfers.*

Proof. see Appendix A.2. □

Theorem 5 completely characterizes the SPNE actions of all SCDG participants when the SC entities are in disadvantage and their budgets are significantly smaller than the total budget of the TO. In this case, the TO allocates budget to both the physical and social games. In response the SC entity with the highest preallocated defense budget $(c_i, i \in \{1,2\})$ chooses to transfer budget to its SC ally.

Theorem 6. *For the SCDG where* $\phi_1 = |\Theta_1| \cdot v_1$ *is the value of the physical CBG,* $\phi_2 = |\Theta_2| \cdot v_2$ *is the value of the cyber-social CBG and prior to the third game stage:*

- *the available budget of the ESA is* $d_1 = c_1 - r$
- *the available budget of the ICT agency is* $d_2 = c_2 + r$
- *the total available budget of the TO* T *is* τ*, and*

- $\frac{2}{|\Theta_1|} < \frac{\tau-\delta(r)}{d_1(r)} < 1$ *and* $\frac{2}{|\Theta_2|} < \frac{\delta(r)}{d_2(r)} < 1$

where $\delta = \sqrt{\frac{\phi_2 d_1 d_2}{\phi_1}}$*, then the second SCDG stage equilibrium strategy for the TO that maximizes its payoff is:*

$$\tau_1^* = T^*(r^{1\to 2}, r^{2\to 1}) = T^*(r) = \tau - \sqrt{\frac{\phi_2 d_1 \cdot d_2}{\phi_1}} \qquad (6.17)$$
$$\tau_2^* = \tau - \tau_1^*$$

In this case the first SCDG stage equilibrium strategies for the two SC entities that maximize their payoff are:

$$R^{*1} = r^{*1\to 2} = \begin{cases} \frac{\frac{\phi_2\cdot(c_1+c_2)^2}{4\phi_1\cdot\tau^2}\cdot c_1 - c_2}{1+\frac{\phi_2\cdot(c_1+c_2)^2}{4\phi_1\cdot\tau^2}}, & if \quad \frac{c_1+c_2}{2\tau} > \sqrt{\frac{\phi_1 c_2}{\phi_2 c_1}} \\ 0, & otherwise \end{cases} \qquad (6.18)$$
$$R^{*2} = r^{*2\to 1} = 0$$

and there exists a SCDG SPNE family of $\{T^*, R^{*1}, R^{*2}\}$ *as defined above. For the case where the budget strength relation of the two SC allies in comparison to the TO is interchanged the same SPNE family exists with the reverse budget transfers.*

Proof. see Appendix A.3. □

Theorem 6 completely characterizes the SPNE actions of all SCDG participants when one SC entity is at disadvantage with fewer resources that its opponent TO, while its ally has a larger budget than the TO. In this case, the TO allocates budget to both physical and social games taking into account the strength of the two opponents along with the significance of each fight. In response, the SC entity with the superior preallocated defense budget ($c_i, i \in \{1,2\}$) in comparison to the TO can transfer budget to its SC ally. The existence and exact amount of the transfer should ensure the safety of this entity's plane and it takes place only if it leads to a higher expected utility for both SC players (higher number of expected wins).

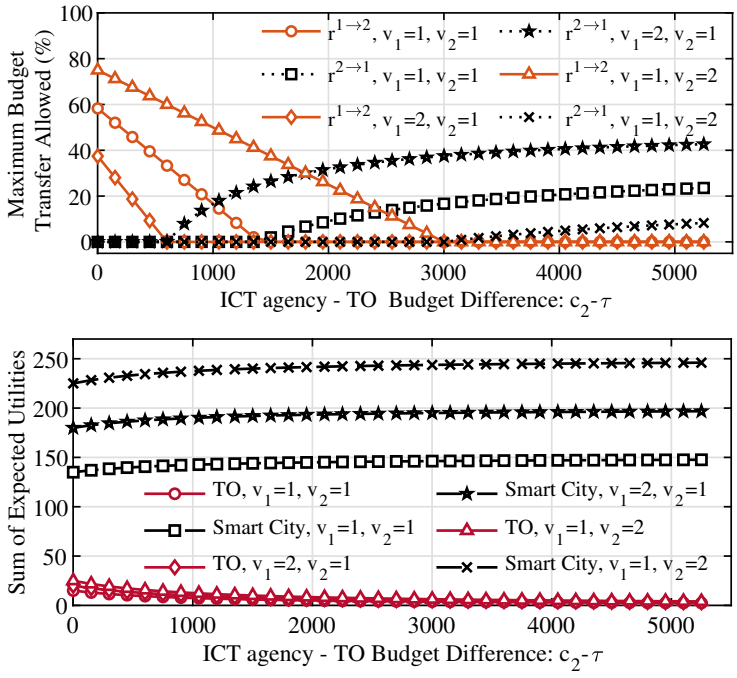


Figure 6.2 TO in budget disadvantage: (Top) Budget transfer among agencies and (Bottom) Expected Utility vs ICT agency budget

6.4 Numerical Evaluation and Discussion

In this section, we present a numerical evaluation of the SCDG focusing on the players' actions and response curves for various game parameters and budget strength relations among all parties. In addition, we will present how the deviation from equilibrium strategies affects the payoffs of the defensive SC players towards compromising the public safety in the examined smart city setting.

6.4.1 SCDG Analysis

First, we focus on the case where both SC entities have greater defense budgets than their adversary TO in an SC setting that consists of $|\Theta_1| = 50$ physical battlefields and $|\Theta_1| = 100$ cyber-social battlefields. We consider a TO whose initial budget is $\tau = 200$, an SC ESA with initial budget $c_1 = 800$, and evaluate how the maximum allowed transfer amount between the SC entities changes as the budget difference between the ICT agency and the

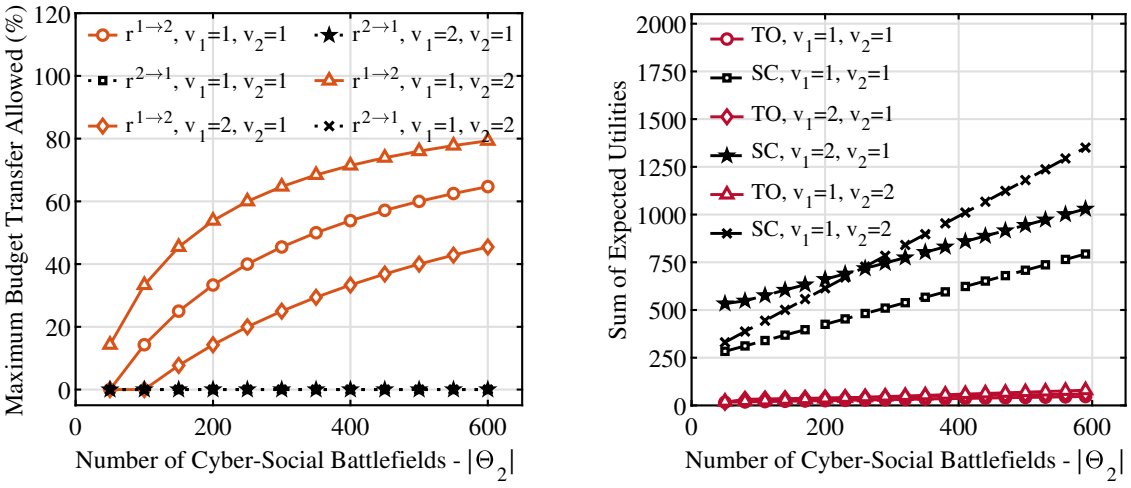
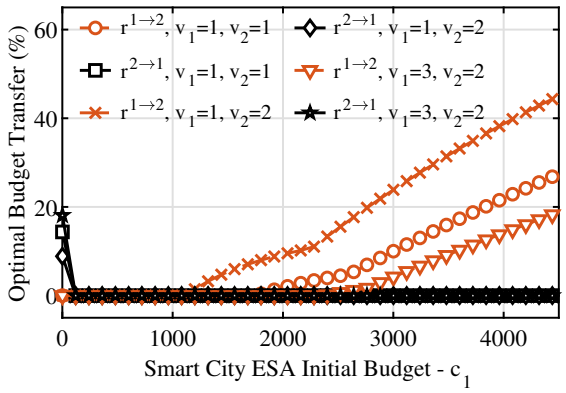


Figure 6.3 TO in budget disadvantage: (Right) Budget transfer among agencies, and (Left) Expected Utility vs Social battlefields Number

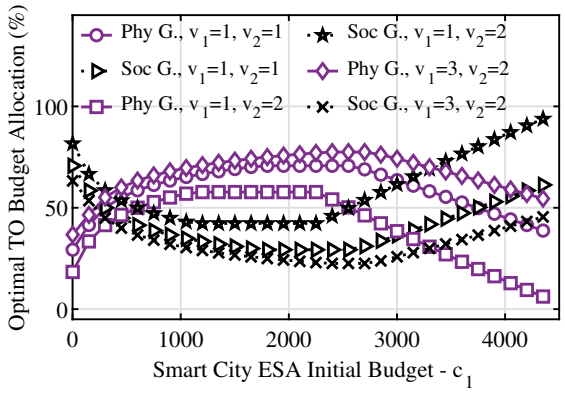
TO increases. Fig. 6.2a shows these results for different game values, namely when a) the physical battles are more important for the two opponents ($\nu_1 > \nu_2$), b) the social battles are critical for the two opponents ($\nu_1 < \nu_2$), or both planes are equally important ($\nu_1 = \nu_2$). We observe that for small budget differences the ESA makes a transfer to the ICT agency up to a certain point that depends on the value of each game/plane. After this point, the TO chooses to allocate all his budget to fight the cyber-social battle therefore a budget transfer from the ICT to the ESA is now optimal for the SC defense. We also observe that the SC entity transferring resources is not always the one with the highest budget but the one with the minimum $\frac{\phi_i}{c_i}$, $i \in \{1,2\}$ value, as sometimes the resourceful agency may have SC battlefields of higher importance to fight for.

In Fig. 6.2b for the same set of parameters we observe how the expected utility of the TO and the expected utility of the SC as a whole (both agencies) changes as the budget of the ICT agency increases. Note that in the context of the two CBGs the expected utility is analogous to the total number of physical and cyber-social battlefields that were won by each player (successfully attacked by the TO, or successfully defended by the SC agencies).

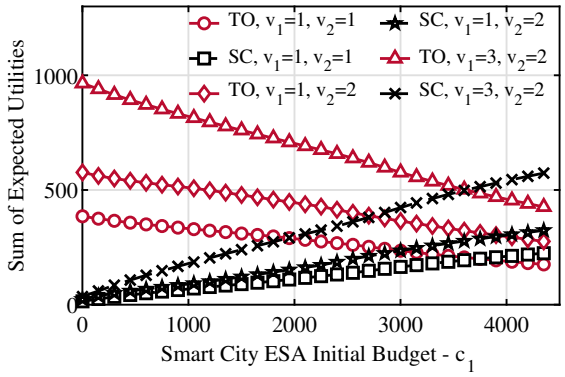
In Fig. 6.3 we evaluate how the SC agencies' budget transfer (Fig. 6.3a), and expected utilities (Fig. 6.3b) change as the number of cyber-social battlefields increases. The number



(a) SC Agencies' Optimal Budget Transfer



(b) TO's Optimal Budget Allocation across Games

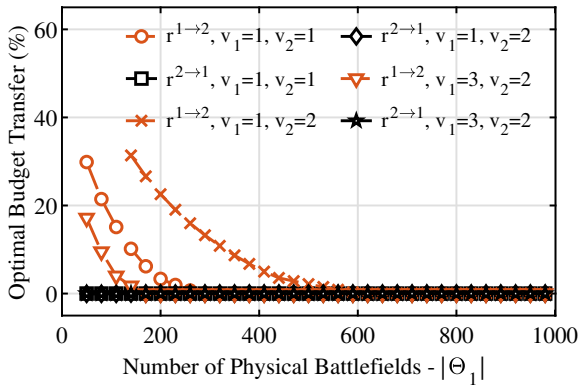


(c) Players' Expected Utilities

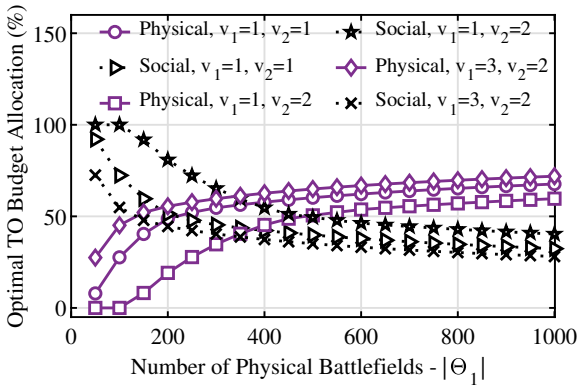
Figure 6.4 Smart City Defense Game Strategies vs ESA Initial Budget

of physical battlefields is $|\Theta_1| = 250$, while the initial budgets for the TO, ESA and ICT agency are $\tau = 200,\ c_1 = 1500,\ c_2 = 300$, respectively. Evidently, the budget of the ESA prohibits the TO from allocating any resources to the physical fight, therefore we observe transfers only from the ESA to the ICT agency whose amount increases as the number of social fights increases. Those transfers lead to a higher expected utility sum for the SC as seen in Fig. 6.3b in comparison to the TO whose limited resources reduce the probability of landing successful attacks.

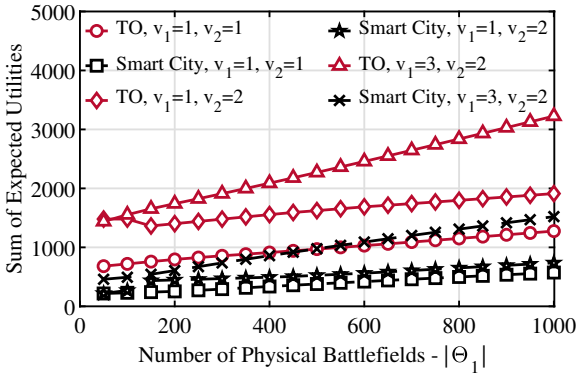
Next, we examine the case where the TO has an advantage in comparison to at least one of the SC agencies. In Fig. 6.4 we consider a SC setting of $|\Theta_1| = 200$ physical and $|\Theta_2| = 200$ cyber-social targets and a TO with available budget of $\tau = 3500$ which is always larger



(a) SC Agencies' Optimal Budget Transfer



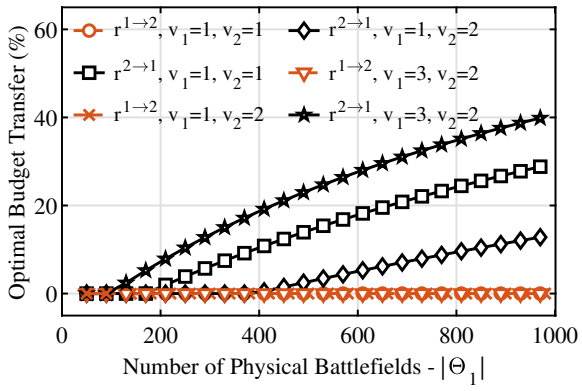
(b) TO's Optimal Budget Allocation across Games



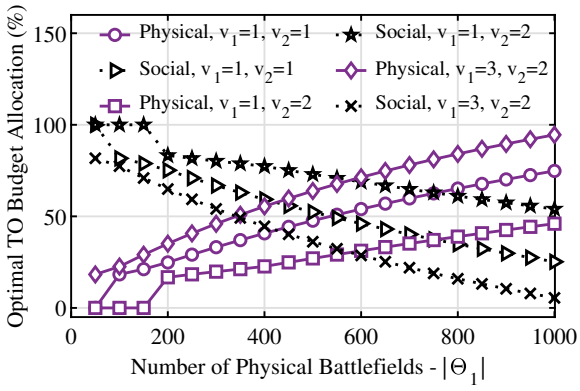
(c) Players' Expected Utilities

Figure 6.5 Smart City Defense Game Strategies vs Number of Physical Battlefields ($\tau = 1000,\ c_1 = 500,\ c_2 = 150$)

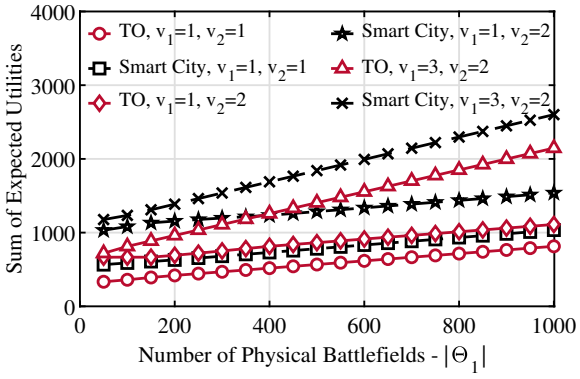
than the initial budget of the ICT agency which is $c_2 = 300$. In this case, we examine how increasing the initial budget c_1 of the ESA affects the SPNE strategies for various target values v_1, v_2. Fig. 6.4a shows how the optimal budget transfer among organizations changes. Initially, the ICT agency transfers budget to the ESA, while as the latter becomes more resourcefully the opposite transfer takes place. Accordingly, Fig. 6.4b shows how the TO responds to the budget transfer between the two agencies. Initially, since the ICT agency has more budget available, the majority of the TO's budget is allocated to the social battlefields. As the budget of the ESA increases the TO allocates less budget to attack the social targets in an attempt to counter the stronger opponent at the physical plane. This behavior that



(a) SC Agencies' Optimal Budget Transfer



(b) TO's Optimal Budget Allocation across Games



(c) Players' Expected Utilities

Figure 6.6 Smart City Defense Game Strategies vs Number of Physical Battlefields ($\tau = 1000,\ c_1 = 150,\ c_2 = 1200$)

maximizes the expected number of wins in the two types of targets, stops after a critical point where the ESA initial budget is significantly greater than the TO's budget. After this point (see Fig. 6.4b) the TO starts allocating more budget to the social game as now this where the SC is vulnerable. Finally, Fig. 6.4c shows the sum of expected utility for the TO and the SC in general. As the total SC defense budget increases so does its expected utility, namely the number of social and physical spaces that will be successfully defended.

Next, in Fig. 6.5,and Fig. 6.6, we evaluate how the SCDG SPNE strategies change as the TO decides to perform attacks against an increasing number of physical targets, while the social spaces under attack remain constant with $|\Theta_2| = 200$. Two different cases are

considered. In Fig. 6.5 the TO has greater initial budget than his two opponents with $\tau = 1000$, $c_1 = 500$, and $c_2 = 150$. When the number of physical targets under attack is small we observe a budget transfer (see Fig. 6.5a) from the resourceful SC entity (here the ESA) to its ally. This transfer is, however, decreasing when the number of physical battlefields grows significantly. The TO's optimal budget allocation is seen in Fig. 6.5b, while in Fig. 6.5c we observe the expected number of won battles for the SCDG opponents. Evidently, the TO initially allocates more resources to the weaker opponent. As the number of his physical targets increases, it is forced to increase the budget allocation towards the physical CBG. Finally, as seen in Fig. 6.5c, the initial budget advantage of the TO ($\tau > c_1, \tau > c_2$) is a significant factor as it always leads to a greater sum of expected utility and therefore a greater number of successful hits. In this case, the budget transfers between the two SC entities described by the SPNE strategies is the optimal response that will minimize losses in both SC planes.

On the contrary, in Fig. 6.6 we examine the case where the ICT agency has a greater budget than both the TO and the ESA. Again, budget transfer (see Fig. 6.6a) occurs to reinforce the weaker SC player. In addition, as the weakest ally has to defend an increasing number of physical targets, the optimal budget transfer percentage from his ally increases as well. In response, as seen in Fig. 6.6b the TO allocates larger budget amounts to the physical fight as the number of the physical targets under attack increases. Finally, Fig. 6.5c shows the sum of expected utilities for the TO and the SC (combined utility of the two agencies) for this specific parameter set as the number of physical targets increases.

6.4.2 Comparative Analysis

In this subsection we present comparative results that showcase how the deviation from the SPNE strategies for the two SC entities affect their utilities, and ability to defend physical and social targets, introducing vulnerabilities into the SC setting. In what follows we consider three budget transfer strategies, between SC allies, namely:

1. no budget transfer occurs
2. a random transfer between between the ESA and the ICT agency takes place
3. both SC agency act accordingly to the SCDG SPNE strategies

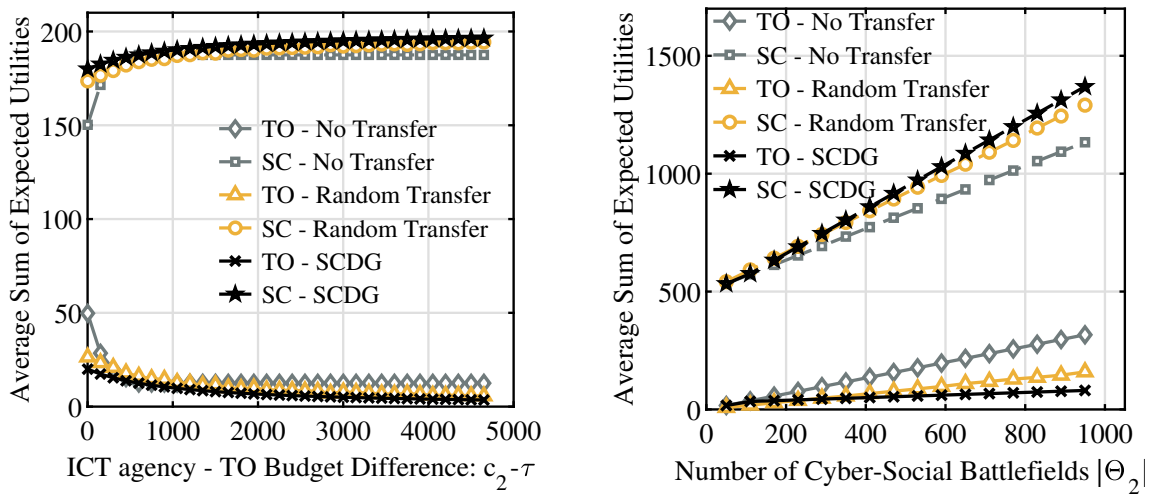


Figure 6.7 Average Sum of Expected Utilities vs (Left) ICT agency initial budget, (Right) Number of Cyber-Social Battlefields

For these cases, we present the average sum of expected utilities. While for the case (a), and (c) the results are analytical, for the random transfer we averaged the sum of expected utilities from 10^4 simulations. Again we will examine different cases regarding the initial budget strength relations among SCDG players.

First, the case where the TO is in a budget disadvantage. In Fig. 6.7a a SC setting with $|\Theta_1| = |\Theta_2| = 100$ physical and social targets is considered with their values being equal $v_1 = v_2 = 1$. The initial budget of the TO and ESA is $\tau = 200$, and $c_1 = 800$ respectively. We present the average sum of expected utilities as the budget of the ICT agency increases in relation to the TO total budget. Evidently, when the SCDG strategies are followed by the SC is the highest (more successfully defended socio-physical targets) while the opposite happens for the TO. The same behavior is observed in Fig. 6.7a where in the same setting, ICT's budget is set to $c_2 = 400 > \tau$, and the average sum of expected utilities is evaluated against an increasing number of social spaces targeted by the TO.

Next we consider the case where the TO has greater budget than at least one opponent in a SC setting where $|\Theta_1| = |\Theta_2| = 800$, $v_1 = v_2 = 1$. Fig. 6.8a shows the average sum of expected utilities as the ESA's initial budget increases, for the case where $\tau = 3500$ and $c_2 = 1000$. Fig. 6.8b shows again the average utilities when the TO decides to target an

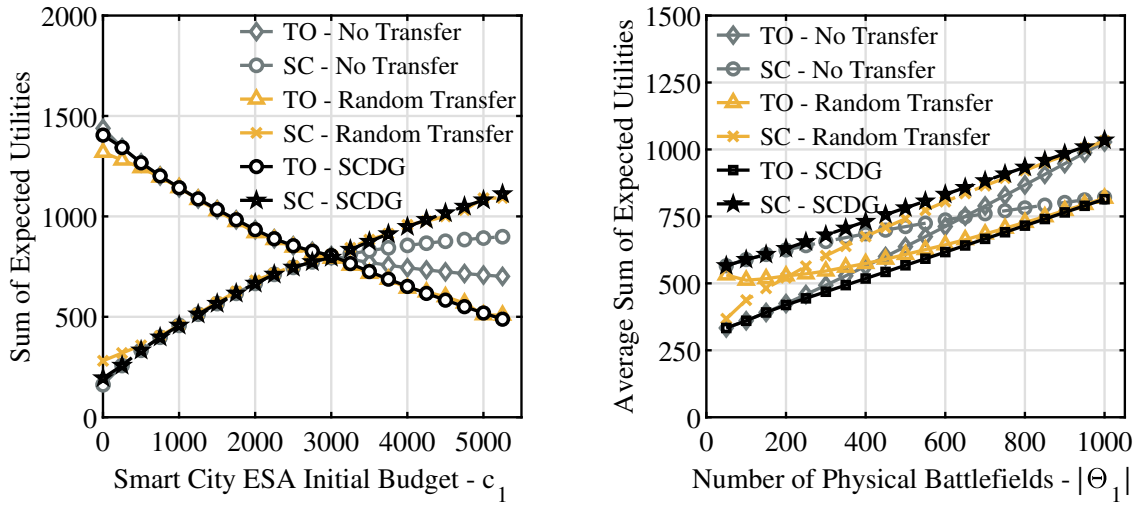


Figure 6.8 Average Sum of Expected Utilities vs (Left) ESA Initial Budget ($\tau = 3500,\ c_2 = 1000$), (Right) Number of Physical Battlefields ($\tau = 1000,\ c_1 = 150,\ c_2 = 1200$)

increasing number of physical targets and the budget of the TO, ESA, and ICT agency are $\tau = 1000,\ c_1 = 150,\ c_2 = 1200$, respectively. Evidently, in both cases, the SCDG strategies for the two SC entities lead to a larger number of successfully defended socio-physical targets than the alternatives. Finally, Fig. 6.9 shows the average expected utilities for each SC entity separately as the number of physical targets under attack increases and player's budget strength are $\tau = 1000,\ c_1 = 500,\ c_2 = 150$. This figure showcases an important property of the SCDG. For the ICT agency, a random transfer yields a higher expected utility/number of wins. However, the SPNE strategy forbids the two SC allies from making a budget transfer. This happens because the proposed game allows budget transfers only if they are beneficial for both allies, and increase their expected wins in both social and physical city battlefields. In our case when a random budget transfer is considered the average expected utility of the ESA is lower than the SPNE strategy of the SCDG, thus randomicity is not beneficial for both allies and both SC planes.

6.5 Related Work

Previous research in the general area of anti-terrorism conflicts utilizes game theory (security games) to model interaction between a defender and a sophisticated attacker [251].

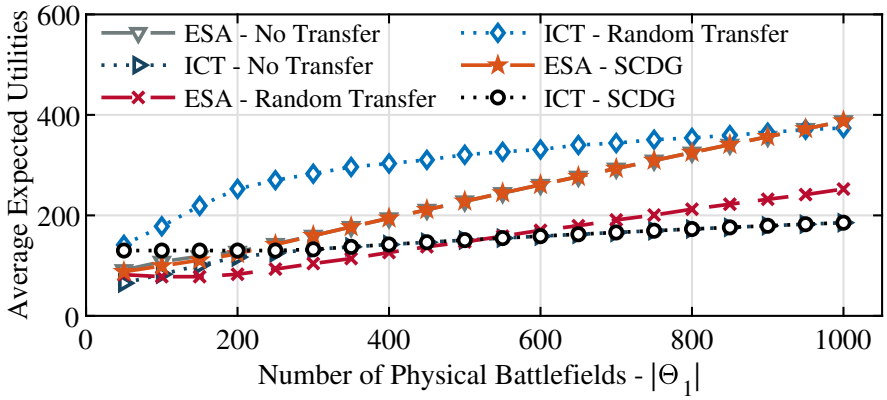


Figure 6.9 Average Expected Utilities for SC Agencies vs Number of Physical Battlefields ($\tau = 1000,\ c_1 = 500,\ c_2 = 150$)

The common assumption in these works is this of the passive defender that allocates resources before any attack without actively harming his adversary. In this context, two cases can be distinguished: (a) the attacker is not aware of the defender's play, and (b) he has complete knowledge. In the first case, the majority of games are simultaneous yielding Nash equilibria in mixed strategies where both players randomize over their actions to confuse their opponents. The most popular game in this category is the Colonel Blotto game, and its numerous variations, where the players allocate finite resources over multiple battlefields [243]. Similarly the work in [21] considers a one-to-one resource allocation game across multiple locations with a mixed-strategy equilibrium where the terrorist can choose between attacking with a suicide bomber or use conventional force. In [29], the authors develop mixed strategies for the two opponents that choose between two actions for each target, namely act (attack or defend) or not. The authors investigate single or multiple-period security games to examine ongoing conflicts where the terrorist can use one or several attack technologies with different capabilities.

However, game-theoretic frameworks should account for the fact that terrorist strategies can adopt in response to the defender's actions, while the interactions between the two opponents are independent. Thus, the second category of research works assumes complete knowledge among the two parties and utilizes multi-stage games that are solved using backward induction yielding sub-game perfect Nash equilibria (SPNEs). In [32] the authors model a two-stage Stackelberg game (leader-follower game) where the state initially decides

where to locate resource-packed facilities and the terrorist, given these locations, decides on the attack targets that will maximize the inflicted damage. The work in [195] extends this model to account for disruption in the defender's facilities with a non-zero probability of failures on the supply-side (resource unavailability) and propose a heuristic algorithm to solve the developed problem.

In our study, a mixed approach is followed where a stage of resource allocation/preparation (pure strategies) precedes the actual allocation among targets modeled as a Colonel Blotto game (mixed strategies). In addition, our model considers two defenders and the creation of a coalition among them. In a similar fashion, the authors in [46] present a multi-stage sequential game model in which a set of different countries are confronted by an international terrorist organization. Initially, countries invest resources to fight proactively the adversary (1^{st} stage), next all countries allocate defense resources (2^{nd} stage), and finally, the terrorist allocates attacking resources among countries (3^{rd} stage). The game studies the nation's cooperation against the terrorist, and yields an SPNE, while in contrast to our work the defensive measures of a specific country can direct terrorist attacks to other allies (the cooperation is not always beneficial). The opposite case of collusive behavior among attackers is studied by Ray et. al. in [247]. Their work introduces a coalition formation game that investigates the characteristics and the mechanisms of alliance creation among terrorist/hacker organizations against a single defender. Finally, the work in [112] models the case of multiple adversaries against a single defender as a Stackelberg security game (defender $\equiv$ leader, attackers $\equiv$ followers), and calculates the optimal defense strategy given knowledge of payoff matrices, and target-related attack-success probabilities.

Other research works that focus on smart city security do so by considering a cyber-physical system perspective with the adversary attempting to compromise individual components. In [94] the authors develop a game theoretic framework to defend intelligent transportation systems against indirect attacks carried out through the power grid. In [95] the authors model CPS elements of a smart city as connected nodes using graph theory and develop a Colonel Blotto-based resource allocation game between a defender and an attacker that tries to compromise the nodes. Similarly, the work in [93] examines an SC's interdependent critical infrastructure (ICI) consisting of power-gas-water distribution systems and considers a two-stage attack to a set of ICI sensor's protection and state estimation quality. The attacker-defender interaction is modeled as a Colonel Blotto alloca-

tion game where the SC administrator allocates resources with the form of computational, communication or financial resources to establish protection levels for the ICI nodes. The authors derive a Mixed Strategy Nash Equilibrium (MSNE) for the two players and examine the optimal defender's strategy for a series of different cases. In [126] the authors formulate a multi-stage Blotto game where a single adversary fights against two defenders. The game focuses on the cyber vulnerability of servers against a hacker, has a hierarchical structure similar to our proposed work, and each defender has to decide whether or not to add additional battlefields to the CB games, or transfer resources to the other player. Finally, the work in [237] examines attacks on the cyber and physical parts of a wide-area network testbed. The attacker chooses to attack a single part, while the defender chooses -or not- to reinforce the whole infrastructure acting according to a game-theoretic framework that yields a pure Nash equilibrium for the two opponents.

6.6 Conclusion

In this chapter, we demonstrate a budget management mechanism between Smart City agencies deployed in cases of simultaneous terrorist attacks on multiple city levels and targets. The Smart City is modeled as a setting with two parallel layers, namely a physical, and a cyber-social. Each layer contains multiple targets/spaces, either physical (e.g., landmarks), or social (e.g., tweeter feeds) and their defense is assigned to two city agencies. A terrorist organization allocates budget to attack both SC layers and as a defense measure, the two agencies make budget transfers between them before allocating their resources among targets. In order to capture their interactions and define the optimal strategies that will maximize the SC defenses, we propose the Smart City Defense Game (SCDG) which is a multi-stage extended form game and derive its sub-game perfect Nash equilibrium. The proposed model provides strategies for budget exchanges between SC allies in cases of terrorist threats by considering the response and resource allocations of the enemy across the two SC planes. We show detailed numerical results for various parameter regions where when the SC agencies act according to the SPNE, they manage to maximize the number of defended targets and minimize the cases where the terrorist organization launches successful attacks.

Chapter 7

Conclusion

This thesis is focused on the use of embedded IoT infrastructures for optimizing public safety services in future Smart Cities. We propose frameworks that incorporate machine learning and game theory to perform passive crowd-sensing for user localization and tracking, prolong the lifetime of critical communication networks, and ensure optimal emergency resource allocation among smart city agencies during multi-target attacks. In this chapter, we summarise our contributions and describe directions for future research.

7.1 Summary of Contributions

In this dissertation, we presented five contributions, each in one chapter. In the second chapter, we documented the BLEBeacon dataset, the first collection of BLE RSSI readings generated by the interaction of mobile users with IoT devices in a realistic smart space environment during a one-month-long IRB-approved trial. In the third chapter, we proposed a localization and user mobility tracking framework that relies on the aforementioned passive RSSI interactions. The framework utilizes unsupervised machine learning to classify each user to a cell location and can adapt over time to any changes in the underlying hardware or environmental landscape changes.

In the fourth chapter, we changed our focus to critical communications and proposed a heterogeneous Public Safety Network (PSN) framework where multiple wireless protocols are utilized to establish device-to-device communications during Smart City emergencies.

The framework manages to prolong the operational lifetime of the user devices via a combination of reinforcement learning-based protocol selection, peer-to-peer clustering, and optimal power control that jointly considers protocol specifications, node distance and social interest, and energy availability. In the fifth chapter, we propose the integration of IoT nodes into public safety networks and present a framework that guarantees energy efficiency for the participating devices through a harvest-transmit-store wireless power communication mechanism, where the IoT nodes harvest energy from the mobile UAV before transmitting their information. The UAV's optimal positioning in the Euclidean 3D space is determined through an optimization problem of maximizing the energy availability of emergency gateway PSN nodes.

Finally, in the sixth chapter, we consider a multi-layer smart city model and present a defense mechanism for optimal SC resource allocation in response to simultaneous terrorist attacks of various types. The Smart City is modeled as a multi-dimensional setting that consists of a lower physical plane and an upper cyber-social one. By considering a Terrorist Organization (TO) attack taking place in both SC layers, we model the optimal response of two SC agencies responsible for public safety and SC defense, namely an Emergency Service Agency (ESA) operating at the physical layer and an Information and Communication Technology (ICT) agency operating at the Cyber-Social SC plane. Each organization aims to deploy its financial resources optimally across multiple spaces of interest either physical or cyber, by also considering the possibility of budget exchange with the other agency. To fully capture the inter-dependencies and interactions among all the conflicting parties we introduce a multi-stage Smart City Defense Game (SCDG) with observed actions and compute the game's subgame perfect Nash equilibrium that describes the optimal strategies of all players focusing on the optimal budget exchange among the SC agencies that minimizes the expected number of successful TO attacks across the two SC layers and targets.

7.2 Future Research Directions

This thesis opens up interesting technical and theoretical directions for several future extensions and research topics. Below we present some of them:

- Our experimental trial can be extended to a larger scale that can go beyond a single university building to a campus scale. Smart City testbeds [176] can indeed answer important research questions on which wireless technologies should be utilized more frequently, and how data extracted by residents should be analyzed [286]. Concerning our work, an extended campus study can reveal the applicability of other passive advertising (e.g., WiFi probe request frames [182]) for similar localization services, and the effect that an outdoor environment will have on RSSI measurements due to different physical obstacles to the radio wave propagation.

- Another possible extension for utilizing the mining of wireless interactions between users and IoT nodes is their use to extract social graphs between them. Indeed, ambient WiFi readings have been used for crowd estimation [305], to classify users into crowdflow [136] (e.g., for urban-flow monitoring and shopping-recommendation), and pedestrian flow estimation [140]. Another related application is event management through the extraction of spatiotemporal patterns from probe requests (e.g., as in [342] where mobile device trajectories are extracted from probe requests and temporal visiting patterns are extracted using k-means and k-shape clustering). Finally, in [299] the authors investigate how WiFi association logs archived by a managed campus network can be used to infer social interactions between students. This logic of inferring social structure from spatiotemporal readings in a smart city can be extended to include apart from mobile users, the IoT nodes, and the extended IoT infrastructure in general (Social Internet of Things [51]). The uses of real-time inference of a social structure within an IoT network (that consists of both edge nodes and user devices) are manifold and such relationships can be used to increase energy efficiency within the wireless network (e.g., see our work in [274, 275] where the node's social relations are utilized to achieve better clustering and energy availability), or even achieve social resilience (i.e., the capability of an IoT network to resist to possible attacks by malicious agents [103]). To this end, the presented BLEBeacon dataset can be utilized as a real-world case study of actual social interactions through spatiotemporal relations between edge devices and mobile occupants.

- Blockchain is among the technologies that are being considered to further support services in a future Smart City, especially when it comes to security and trust [105,

129]. The number of possible application vectors has already exploded as we see practical use of blockchains in energy trading [125] and local energy markets (see our work in [67]), for IoT/Smart Grid data protection [90, 262], for authentication, registration, and management of participatory IoT devices [131] or even as a building block for software-defined networking in smart cities [23]. Works like IoTShare [131] use blockchains to deploy network-on-demand instances on top of the IoT infrastructure within a smart city for supporting emergency relief management, surveillance, traffic control, and other public safety-critical applications. Such integration of blockchain technology into IoT infrastructures still presents several challenges that create room for future research. First, any related application should be developed with power conservation in mind as typically IoT devices rely on limited resources. Next, while most related works assume that IoT nodes will volunteer to participate in such distributed frameworks [131], this is rarely the case in practice. Thus, an interesting research thrust would be the development of incentive mechanisms for blockchain-based IoT applications. Recently more and more works utilize edge computing to allow for IoT nodes to offload resources (network, computation, storage, etc.) while ensuring participation incentives with limited use of local resources and using peer-to-peer reputation exchange schemes [57]. Finally, the integration of distributed ledger technologies in IoT networks requires the careful study of both storage and communication link limits. In the case of storage, future research should focus on an optimal distributed ledger structure that will retain the blockchain integrity with limited storage overhead. Finally, it would be worth investigating how a blockchain-based IoT network scales under different bandwidth availability or different backhaul technologies – e.g., broadband (bandwidth: 10s of Mbps), cellular (100s of kbps), or mesh (10s of kbps) –. For instance, could a set of IoT nodes carrying cellular kits (e.g., [16, 122]) sustain a blockchain-based framework? For comparison, usually, latency for DSL modems is in the tens of milliseconds (10 to 70 ms) while for cellular links an order of magnitude larger (100 to 700 ms) without accounting for the upcoming involvement of 5G that will bring big improvements in latency (20-30 ms practically).

- Finally, the recent advances in practical quantum computing (a possibility within 20 years) coupled with the massive adoption of IoT raises serious security concerns

among IT professionals. The proven ability of a quantum computer to solve elliptic curve discrete logarithm/integer factorization problems poses a threat to current digital signatures and public-key cryptography (RSA, ECC, ECDSA) [18, 19, 199]. Consequently, NIST initiated an open call for quantum-resistant crypto algorithms, that yielded the next generation of quantum-secure algorithms for key exchange and authentication [216], focusing on security guarantees, and treating performance as a future goal. Since the post-quantum (PQ) algorithms present significant differences (key generation times, key/signature sizes), they should not be evaluated out-of-context. While multiple works evaluate the performance of the new quantum-resistant schemes in terms of browser latency impact [175, 219, 267, 268], and even ARM Cortex-M4 energy requirements [250], there is still room for investigating the impact of these novel schemes on IoT networks and in extension smart cities. Evidently, the resilience of the future smart city infrastructure and information security will greatly depend on the successful and widespread adoption of these schemes in case quantum computers become available.

References

[1] *3GGP - 3rd Generation partnership program*. accessed on Mar. 22, 2018. URL: `http://www.3gpp.org` (visited on 03/22/2018).

[2] *A Pathway to the Distributed Grid*. Tech. rep. SolarCity, 2016.

[3] *A Stronger, More Resilient New York*. Tech. rep. PlaNYC, 2013.

[4] Ahmed, A et al. "Cyber physical security analytics for anomalies in transmission protection systems". *2018 IEEE Industry Applications Society Annual Meeting (IAS)*. IEEE. 2018, pp. 1–8.

[5] Ahmed, N. et al. "A survey of covid-19 contact tracing apps". *IEEE Access* **8** (2020), pp. 134577–134601.

[6] *Airbnb's open homes program: Opening homes in times of crisis*. `https://www.airbnb.org`.

[7] Akhavan, Z., Esmaeili, M., Sikeridis, D. & Devetsikiotis, M. "Internet of Things-enabled Passive Contact Tracing in Smart Cities". *Internet of Things* (2021), p. 100397.

[8] Albrecht, M. R., Degabriele, J. P., Hansen, T. B. & Paterson, K. G. "A surfeit of SSH cipher suites". *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 2016, pp. 1480–1491.

[9] Alexander, R. *The Safe City: Assessing Opportunities and Challenges in a Budding Security Concept*. `https://ihsmarkit.com/research-analysis/the-safe-city-assessing-opportunities-and-challenges.html`.

[10] Ali, K. et al. "Architecture for public safety network using D2D communication". *Wireless Communications and Networking Conference (WCNC), 2016 IEEE*. IEEE. 2016, pp. 1–6.

[11] Alkim, E., Ducas, L., Pöppelmann, T. & Schwabe, P. "Post-quantum key exchange—a new hope". *25th {USENIX} Security Symposium ({USENIX} Security 16)*. 2016, pp. 327–343.

[12] Alletto, S. et al. "An indoor location-aware system for an IoT-based smart museum". *IEEE Internet of Things Journal* **3**.2 (2016), pp. 244–253.

[13] Almoqbel, M. & Xu, S. "Computational Mining of Social Media to Curb Terrorism". *ACM Computing Surveys (CSUR)* **52**.5 (2019), pp. 1–25.

[14] Alsamhi, S. H., Ma, O., Ansari, M. S. & Almalki, F. A. “Survey on collaborative smart drones and internet of things for improving smartness of smart cities”. *IEEE Access* **7** (2019), pp. 128125–128152.

[15] Androulaki, E. et al. “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains”. *Proceedings of the Thirteenth EuroSys Conference*. EuroSys ’18. ACM, 2018, 30:1–30:15.

[16] Anguera, J et al. *Virtual Antenna provides mobile and GPS connection in the Thingy: 91 cellular IoT module*. `https://cdn.everythingrf.com/live/Virtual_Antenna_for_Thingy91.pdf`.

[17] *Annual Energy Outlook 2020*. Tech. rep. U.S. Energy Information Administration, 2020.

[18] ANSI. *The Elliptic Curve Key Agreement and Key Transport Protocols*. American National Standards Institute, X9-Financial Services. 1999.

[19] ANSI. *ANSI X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*. American National Standards Institute, X9-Financial Services. 2005.

[20] Apple. *Getting Started with iBeacon*. 2014. URL: `https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf`.

[21] Arce, D. G., Kovenock, D. & Roberson, B. “Weakest-link attacker-defender games with multiple attack technologies”. *Naval Research Logistics (NRL)* **59**.6 (2012), pp. 457–469.

[22] Athukoralage, D., Guvenc, I., Saad, W. & Bennis, M. “Regret based learning for UAV assisted LTE-U/WiFi public safety networks”. *Global Communications Conference (GLOBECOM)*. IEEE. 2016, pp. 1–7.

[23] Aujla, G. S. et al. “Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications”. *IEEE Network* **34**.2 (2020), pp. 83–91.

[24] Aumasson, J.-P. et al. *SPHINCS+ - Submission to the 2nd round of the NIST post-quantum project*. `https://sphincs.org/data/sphincs+-round2-specification.pdf`. Specification document (part of the submission package). 2019.

[25] Bahl, P. & Padmanabhan, V. N. “RADAR: An in-building RF-based user location and tracking system”. *Proc., IEEE INFOCOM*. 2000, pp. 775–784.

[26] Baldini, G., Karanasios, S., Allen, D. & Vergari, F. “Survey of wireless communication technologies for public safety”. *IEEE Communications Surveys & Tutorials* **16**.2 (2014), pp. 619–641.

[27] Barbose, G. et al. *Tracking the Sun: Pricing and Design Trends for Distributed Photovoltaic Systems in the United States 2019 Edition*. Tech. rep. Lawrence Berkeley National Laboratory, 2019.

[28] Barka, E. et al. “UNION: a trust model distinguishing intentional and UNIntentional misbehavior in inter-UAV communicatiON”. *Journal of Advanced Transportation* **2018** (2018).

[29] Baron, O., Berman, O. & Gavious, A. “A Game between a Terrorist and a Passive Defender”. *Production and Operations Management* **27**.3 (2018), pp. 433–457.

[30] Bay, J. et al. “BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders”. *Government Technology Agency-Singapore, Tech. Rep* (2020).

[31] Behnezhad, S. et al. “Faster and Simpler Algorithm for Optimal Strategies of Blotto Game.” *AAAI*. 2017, pp. 369–375.

[32] Berman, O. & Gavious, A. “Location of terror response facilities: A game between state and terrorist”. *European Journal of Operational Research* **177**.2 (2007), pp. 1113–1133.

[33] Bi, S., Zeng, Y. & Zhang, R. “Wireless powered communication networks: An overview”. *IEEE Wireless Communications* **23**.2 (2016), pp. 10–18.

[34] Bindel, N., Herath, U., McKague, M. & Stebila, D. “Transitioning to a quantum-resistant public key infrastructure”. *Proc. 8th International Conference on Post-Quantum Cryptography (PQCrypto) 2017*. Ed. by Lange, T. & Takagi, T. LNCS. To appear. Springer, 2017.

[35] Boeyen, S. et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280. 2008.

[36] Bos, J. et al. “CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM”. *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. 2018, pp. 353–367.

[37] Bos, J. W., Costello, C., Naehrig, M. & Stebila, D. “Post-quantum key exchange for the TLS protocol from the ring learning with errors problem”. *2015 IEEE Symposium on Security and Privacy*. IEEE. 2015, pp. 553–570.

[38] Bousquet, C. “Data-Driven Emergency Response: Learning from Hurricanes Harvey and Irma”. *Data-Smart City Solutions, October* **3** (2017).

[39] Bronski, P. et al. *The Economics of Grid Defection*. Tech. rep. Rocky Mountain Institute, 2014.

[40] Buchmann, J. A., Butin, D., Göpfert, F. & Petzoldt, A. “Post-quantum cryptography: state of the art”. *The New Codebreakers*. Springer, 2016, pp. 88–108.

[41] Burke, J. “The Age of Selfie Jihad: How Evolving Media Technology Is Changing Terrorism”. *CTC Sentinel* **9**.11 (2016), pp. 1–8.

[42] Buterin, V. *"Another category of use cases is verifying integrity of processes. For example, in an auction, you might want to verify that everyone's bid that was submitted on time was included, and no late bids were included. If bids are published to chain, even encrypted, you can do this."*. `https://twitter.com/vitalikbuterin/status/1072161050550710272`. Accessed: 2020-2-10. 2018.

[43] Bürstinghaus-Steinbach, K., Krauß, C., Niederhagen, R. & Schneider, M. *Post-Quantum TLS on Embedded Systems*. ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2020). `https://eprint.iacr.org/2020/308`. 2020.

[44] Cabrero, S. et al. “CWI-ADE2016 Dataset: Sensing nightclubs through 40 million BLE packets”. *Proceedings of the 8th ACM on Multimedia Systems Conference*. ACM. 2017, pp. 181–186.

[45] Campagna, M. *Hybrid-Key Exchanges as an Interim-to-Permanent Solution to Cryptographic Agility*. 2019.

[46] Cárceles-Poveda, E. & Tauman, Y. “A strategic analysis of the war against transnational terrorism”. *Games and Economic Behavior* **71**.1 (2011), pp. 49–65.

[47] Cardone, G. et al. “Crowdsensing in urban areas for city-scale mass gathering management: Geofencing and activity recognition”. *IEEE Sensors Journal* **14**.12 (2014), pp. 4185–4195.

[48] *CASE 14-M-0101 - Proceeding on Motion of the Commission in Regard to Reforming the Energy Vision: Notice of Technical Conference Regarding Earnings Impact Mechanisms, Market Based Earnings, Standby Rates and Related Issues*. Tech. rep. Department of Public Service, State of New York, 2016.

[49] *CASE 14-M-0101 - Proceeding on Motion of the Commission in Regard to Reforming the Energy Vision: Staff White Paper on Ratemaking and Utility Business Models*. Tech. rep. Department of Public Service, State of New York, 2015.

[50] Catteeuw, D. & Manderick, B. "Learning in the time-dependent minority game". *Proceedings of the 11th Annual Conference Companion on Genetic and Evolutionary Computation Conference: Late Breaking Papers*. ACM. 2009, pp. 2011–2016.

[51] Cauteruccio, F. et al. "An approach to compute the scope of a social object in a Multi-IoT scenario". *Pervasive and Mobile Computing* **67** (2020), p. 101223.

[52] Chai, X. & Yang, Q. "Reducing the calibration effort for probabilistic indoor location estimation". *IEEE Trans. Mobile Comput.* **6**.6 (2007), pp. 649–662.

[53] Chakraborty, A., Ortiz, L. E. & Das, S. R. "Network-side positioning of cellular-band devices with minimal effort". *Proc., IEEE INFOCOM*. 2015, pp. 2767–2775.

[54] Challet, D., Marsili, M., Zhang, Y.-C., et al. "Minority games: interacting agents in financial markets". *OUP Catalogue, Oxford Univ. Press* (2013).

[55] Chamoso, P. et al. "Smart city as a distributed platform: Toward a system for citizen-oriented management". *Computer Communications* **152** (2020), pp. 323–332.

[56] Chan, C.-l., Fontugne, R., Cho, K. & Goto, S. "Monitoring TLS adoption using backbone and edge traffic". *IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE. 2018, pp. 208–213.

[57] Chatzopoulos, D., Ahmadi, M., Kosta, S. & Hui, P. "Flopcoin: A cryptocurrency for computation offloading". *IEEE transactions on Mobile Computing* **17**.5 (2017), pp. 1062–1075.

[58] Chen, H., Yang, B., Pei, H. & Liu, J. "Next generation technology for epidemic prevention and control: Data-driven contact tracking". *Ieee Access* **7** (2018), pp. 2633–2642.

[59] Chen, X., Li, X., Guo, D. & Grosspietsch, J. "Resource Allocation in Public Safety Broadband Networks With Rapid-Deployment Access Points". *IEEE Trans. on Vehicular Tech.* **67**.2 (2018), pp. 1660–1671.

[60] Chen, Z., Haykin, S., Eggermont, J. J. & Becker, S. *Correlative learning: a basis for brain and adaptive systems*. Vol. 49. John Wiley & Sons, 2008.

[61] Chintalapudi, K., Padmanabha Iyer, A. & Padmanabhan, V. N. "Indoor localization without the pain". *Proc., ACM MobiCom*. 2010, pp. 173–184.

[62] Christidis, K & Devetsikiotis, M. “Blockchains and Smart Contracts for the Internet of Things”. *IEEE Access* **4** (2016), pp. 2292–2303.

[63] Christidis, K. *island-input*. `http://dx.doi.org/10.5281/zenodo.3871075`. Accessed: 2019-9-14. 2017.

[64] Christidis, K. *overlap*. `https://doi.org/10.5281/zenodo.3871070`. Accessed: 2019-9-13. 2017.

[65] Christidis, K. *cmap*. `http://dx.doi.org/10.5281/zenodo.3871065`. 2018.

[66] Christidis, K. & Devetsikiotis, M. “Blockchains and smart contracts for the internet of things”. *Ieee Access* **4** (2016), pp. 2292–2303.

[67] Christidis, K., Sikeridis, D., Wang, Y. & Devetsikiotis, M. “A framework for designing and evaluating realistic blockchain-based local energy markets”. *Applied Energy* **281** (2021), p. 115963.

[68] Christidis, K. & Wang, Y. *island*. `http://dx.doi.org/10.5281/zenodo.3871077`. Accessed: 2020-2-10. 2018.

[69] Christidis, K. *dauction*. `http://dx.doi.org/10.5281/zenodo.3871067`. Accessed: 2020-2-18. 2018.

[70] Chu, J., Dukkipati, N., Cheng, Y. & Mathis, M. *Increasing TCP's Initial Window*. RFC 6928. 2013.

[71] Cremers, C. et al. “A comprehensive symbolic analysis of TLS 1.3”. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2017, pp. 1773–1788.

[72] Cremers, C. J. F., Horvat, M., Scott, S. & Merwe, T. van der. “Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication”. *2016 IEEE Symposium on Security and Privacy (SP)* (2016), pp. 470–485.

[73] Crockett, E., Paquin, C. & Stebila, D. “Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH”. *NIST 2nd Post-Quantum Cryptography Standardization Conference 2019*. 2019.

[74] Dawid, A. P. & Skene, A. M. “Maximum likelihood estimation of observer error-rates using the EM algorithm”. *Applied statistics* (1979), pp. 20–28.

[75] Dempster, A. P., Laird, N. M. & Rubin, D. B. “Maximum likelihood from incomplete data via the EM algorithm”. *Journal of the royal statistical society. Series B (methodological)* (1977), pp. 1–38.

[76] Dickinson, P., Cielniak, G., Szymanezyk, O. & Mannion, M. “Indoor positioning of shoppers using a network of Bluetooth Low Energy beacons”. *Indoor Positioning and Indoor Navigation (IPIN), 2016 International Conference on*. IEEE. 2016, pp. 1–8.

[77] Ding, J. et al. *Rainbow - Algorithm Specification and Documentation*. `https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions`. The 2nd Round Proposal. 2019.

[78] Domingos, P. & Pazzani, M. “On the optimality of the simple Bayesian classifier under zero-one loss”. *Machine learning* **29**.2 (1997), pp. 103–130.

[79] Dong, W., Guan, T., Lepri, B. & Qiao, C. “PocketCare: Tracking the flu with mobile phones using partial observations of proximity and symptoms”. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* **3**.2 (2019), pp. 1–23.

[80] Doumi, T. et al. “LTE for public safety networks”. *IEEE Communications Magazine* **51**.2 (2013), pp. 106–112.

[81] Ducas, L. et al. *CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation*. `https://pq-crystals.org/dilithium/resources.shtml`. Submission to round 2 of the NIST post-quantum project. 2018.

[82] Dukkipati, N. et al. “An argument for increasing TCP’s initial congestion window”. *ACM SIGCOMM Computer Communication Review* **40**.3 (2010), pp. 26–33.

[83] Dunlop, J., Girma, D. & Irvine, J. *Digital mobile communications and the TETRA system*. John Wiley & Sons, 2013.

[84] Eames, K. T. & Keeling, M. J. “Contact tracing and disease control”. *Proceedings of the Royal Society of London. Series B: Biological Sciences* **270**.1533 (2003), pp. 2565–2571.

[85] Eckhoff, D. & Wagner, I. “Privacy in the smart city—applications, technologies, challenges, and solutions”. *IEEE Communications Surveys & Tutorials* **20**.1 (2017), pp. 489–516.

[86] Ejaz, W. et al. “Efficient energy management for the internet of things in smart cities”. *IEEE Communications Magazine* **55**.1 (2017), pp. 84–91.

[87] Elizabeth, W. & Saeed, A. *Airbnb hosts are offering free housing to thousands of California wildfire evacuees*. https://edition.cnn.com/2019/10/29/us/california-wildfire-airbnb-free-housing-trnd/index.html.

[88] *European Innovation Partnership on Smart Cities and Communities (EIP-SCC)*. http://ec.europa.eu/eip/smartcities/. 2019.

[89] Faisal, M. "We See You: Terrorist Prediction Framework through Psychological and Social Behaviors". *2020 7th International Conference on Soft Computing & Machine Intelligence (ISCMI)*. IEEE. 2020, pp. 204–212.

[90] Fan, L., Cronemberger, F. & Gil-Garcia, J. R. "Using Blockchain Technology to Manage IoT Data for Smart City Initiatives: A Conceptual Framework and Initial Experiments Based on Smart Contracts". *Beyond Smart and Connected Governments*. Springer, 2020, pp. 85–108.

[91] Faragher, R. & Harle, R. "Location fingerprinting with bluetooth low energy beacons". *IEEE journal on Selected Areas in Communications* **33**.11 (2015), pp. 2418–2428.

[92] Feng, D. et al. "Device-to-device communications in cellular networks". *IEEE Communications Magazine* **52**.4 (2014), pp. 49–55.

[93] Ferdowsi, A., Saad, W. & Mandayam, N. B. "Colonel Blotto Game for Sensor Protection in Interdependent Critical Infrastructure". *IEEE Internet of Things Journal* (2020), pp. 1–1.

[94] Ferdowsi, A., Eldosouky, A. & Saad, W. "Interdependence-Aware Game-Theoretic Framework for Secure Intelligent Transportation Systems". *IEEE Internet of Things Journal* (2020).

[95] Ferdowsi, A., Saad, W., Maham, B. & Mandayam, N. B. "A Colonel Blotto game for interdependence-aware cyber-physical systems security in smart cities". *Proceedings of the 2nd International Workshop on Science of Smart City Operations and Platforms Engineering*. ACM. 2017, pp. 7–12.

[96] Ferdowsi, A., Sanjab, A., Saad, W. & Basar, T. "Generalized Colonel Blotto game". *2018 Annual American Control Conference (ACC)*. IEEE. 2018, pp. 5744–5749.

[97] Ferguson, N. et al. "Report 9: Impact of non-pharmaceutical interventions (NPIs) to reduce COVID19 mortality and healthcare demand". *Imperial College London* **10** (2020), p. 77482.

[98] Ferrara, E. et al. "The rise of social bots". *Communications of the ACM* **59**.7 (2016), pp. 96–104.

[99] Figueiredo, M. A. T. & Jain, A. K. “Unsupervised learning of finite mixture models”. *IEEE Trans. Pattern Anal. Mach. Intell.* **24**.3 (2002), pp. 381–396.

[100] *FirstNet*. `https://www.firstnet.com`.

[101] Floyd, S. *Limited Slow-Start for TCP with Large Congestion Windows*. RFC 3742. 2004.

[102] Fluhrer, S., McGrew, D., Kampanakis, P. & Smyslov, V. *Postquantum Preshared Keys for IKEv2*. Internet-Draft draft-ietf-ipsecme-qr-ikev2-08. Work in Progress. Internet Engineering Task Force, 2019. 18 pp.

[103] Fortino, G., Messina, F., Rosaci, D. & Sarne, G. M. “Resiot: An iot social framework resilient to malicious activities”. *IEEE/CAA Journal of Automatica Sinica* **7**.5 (2020), pp. 1263–1278.

[104] Froomkin, A. M. “Regulating Mass Surveillance as Privacy Pollution: Learning from Environemntal Impact Statements”. *U. Ill. L. Rev.* (2015), p. 1713.

[105] Fu, Y. & Zhu, J. “Trusted data infrastructure for smart cities: a blockchain perspective”. *Building Research & Information* **49**.1 (2021), pp. 21–37.

[106] Fudenberg, D. & Tirole, J. “Game theory, 1991”. *Cambridge, Massachusetts* **393**.12 (1991), p. 80.

[107] Garcia, V. M. et al. “Management of Real-Time Data for a Smart Flooding Alert System”. *2020 IEEE International Smart Cities Conference (ISC2)*. IEEE, pp. 1–8.

[108] Gasser, O., Holz, R. & Carle, G. “A deeper understanding of SSH: Results from Internet-wide scans”. *2014 IEEE Network Operations and Management Symposium (NOMS)*. IEEE. 2014, pp. 1–9.

[109] Gershman, S. J. & Blei, D. M. “A tutorial on Bayesian nonparametric models”. *Journal of Math. Psychology* **56**.1 (2012), pp. 1–12.

[110] *Getting Started with iBeacon*. URL: `https://developer.apple.com/ibeacon` (visited on 01/04/2017).

[111] Ghedini, A. & Vasiliev, V. *TLS Certificate Compression*. Internet-Draft draft-ietf-tls-certificate-compression-10. Work in Progress. Internet Engineering Task Force, 2020. 8 pp.

[112] Gholami, S. et al. “Divide to defend: Collusive security games”. *International Conference on Decision and Game Theory for Security*. Springer. 2016, pp. 272–293.

[113] Gimbal. *Gimbal Proximity Beacon Series 10*. 2017. URL: https://store.gimbal.com/collections/beacons/products/s10.

[114] Girolami, M., Mavilia, F. & Delmastro, F. "Sensing social interactions through BLE beacons and commercial mobile devices". *Pervasive and Mobile Computing* **67** (2020), p. 101198.

[115] Goldie-Scot, L. *A Behind the Scenes Take on Lithium-ion Battery Prices*. https://about.bnef.com/blog/behind-scenes-take-lithium-ion-battery-prices/. Accessed: 2020-1-25. 2019.

[116] Google. *Google Beacon Platform*. 2018. URL: https://developers.google.com/beacons/.

[117] Google. *Google Transparency Report - HTTPS encryption on the web*. https://transparencyreport.google.com/https/overview. Web page. Accessed 2020-06-19. 2020.

[118] Goswami, A., Ortiz, L. E. & Das, S. R. "WiGEM: A learning-based approach for indoor localization". *Proc., ACM CoNEXT*. 2011, 3:1–3:12.

[119] *GridWise Transactive Energy Framework Version 1.0*. Tech. rep. The GridWise Architecture Council, 2015.

[120] *GSMA Internet of Things Case Study: How Cellular Technology Enables Anti-Fire Drones*. https://www.gsma.com/iot/wp-content/uploads/2019/02/GSMA-Anti-fire-Drones-Case-Study.pdf.

[121] *GSMA Internet of Things Case Study: Telefónica's IoT Solution Fights Motorbike Theft*. https://www.gsma.com/iot/wp-content/uploads/2020/04/Telefonica-Honda-Case-Study-Final.pdf.

[122] *GSMA Mobile IoT Modules List*. https://www.gsma.com/iot/mobile-iot-modules.

[123] Guan, R. & Harle, R. "Towards a crowdsourced radio map for indoor positioning system". *Proc., IEEE PerCom Workshops*. 2017, pp. 207–212.

[124] Guan, Z. et al. "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities". *IEEE Communications Magazine* **56**.7 (2018), pp. 82–88.

[125] Guo, J., Ding, X. & Wu, W. "A blockchain-enabled ecosystem for distributed electricity trading in smart city". *IEEE Internet of Things Journal* (2020).

[126] Gupta, A. et al. “A three-stage Colonel Blotto game with applications to cyberphysical security”. *American Control Conference (ACC), 2014*. IEEE. 2014, pp. 3820–3825.

[127] Hajimirsaadeghi, M. & Mandayam, N. B. “A dynamic colonel blotto game model for spectrum sharing in wireless networks”. *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE. 2017, pp. 287–294.

[128] Hajimirsadeghi, M., Sridharan, G., Saad, W. & Mandayam, N. B. “Inter-network dynamic spectrum allocation via a Colonel Blotto game.” *CISS*. 2016, pp. 252–257.

[129] Hakak, S. et al. “Securing smart cities through blockchain technology: Architecture, requirements, and challenges”. *IEEE Network* **34**.1 (2020), pp. 8–14.

[130] *HaMagen - Israeli Health Ministry*. `https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/`. 2020.

[131] Hamdaoui, B., Alkalbani, M., Rayes, A. & Zorba, N. “IoTShare: A Blockchain-Enabled IoT Resource Sharing On-Demand Protocol for Smart City Situation-Awareness Applications”. *IEEE Internet of Things Journal* **7**.10 (2020), pp. 10548–10561.

[132] Hammons, R. & Myers, J. “Smart Cities”. *IEEE Internet of Things Magazine* **2**.2 (2019), pp. 8–9.

[133] Harris III, A. F. et al. “Bluetooth Low Energy in Dense IoT Environments”. *IEEE Communications Magazine* **54**.12 (2016), pp. 30–36.

[134] Harvey, H. & Aggarwal, S. *Rethinking Policy to Deliver a Clean Energy Future*. Tech. rep. Energy Innovation, 2013.

[135] Hassanalieragh, M. et al. “Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges”. *Services Computing (SCC), 2015 IEEE International Conference on*. IEEE. 2015, pp. 285–292.

[136] He, S. & Shin, K. G. “Crowd-flow graph construction and identification with spatio-temporal signal feature fusion”. *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE. 2019, pp. 757–765.

[137] Heydon, R. *Bluetooth low energy: the developer’s handbook*. Prentice Hall, 2013.

[138] Hirsch, M. et al. “The medical response to multisite terrorist attacks in Paris”. *The Lancet* **386**.10012 (2015), pp. 2535–2538.

[139] Hoffman, P. E. *SMTP Service Extension for Secure SMTP over Transport Layer Security*. RFC 3207. 2002.

[140] Huang, B., Mao, G., Qin, Y. & Wei, Y. "Pedestrian Flow Estimation Through Passive WiFi Sensing". *IEEE Transactions on Mobile Computing* (2019).

[141] Hülsing, A., Rijneveld, J., Schanck, J. M. & Schwabe, P. "Ntru-hrss-kem". *NIST submissions* (2017).

[142] Hwang, J. et al. "Interworking Models of Smart City with Heterogeneous Internet of Things Standards". *IEEE Communications Magazine* **57**.6 (2019), pp. 74–79.

[143] Imran, M., Castillo, C., Diaz, F. & Vieweg, S. "Processing social media messages in mass emergency: A survey". *ACM Computing Surveys (CSUR)* **47**.4 (2015), p. 67.

[144] Inaya, M., Meli, M., Sikeridis, D. & Devetsikiotis, M. "A real-subject evaluation trial for location-aware smart buildings". *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2017, pp. 301–306.

[145] Innes, M., Dobreva, D. & Innes, H. "Disinformation and digital influencing after terrorism: spoofing, truthing and social proofing". *Contemporary Social Science* (2019), pp. 1–15.

[146] Inskeep, B et al. *The 50 States of Solar: 2015 Policy Review and Q4 Quarterly Report*. Tech. rep. North Carolina Clean Energy Technology Center & Meister Consultants Group, 2016.

[147] Jeon, K. E., She, J., Soonsawad, P. & Ng, P. C. "BLE Beacons for Internet of Things Applications: Survey, Challenges and Opportunities". *IEEE Internet of Things Journal* (2018).

[148] Jin, D. et al. "Smart street lighting system: A platform for innovative smart city applications and a new frontier for cyber-security". *The Electricity Journal* **29**.10 (2016), pp. 28–35.

[149] Johnson, N., Hui, P., Zheng, D. & Tai, C. "Minority game with arbitrary cutoffs". *Physica A: Statistical Mechanics and its Applications* **269**.2-4 (1999), pp. 493–502.

[150] Jung, S. H., Moon, B.-C. & Han, D. "Performance Evaluation of Radio Map Construction Methods for Wi-Fi Positioning Systems". *IEEE Transactions on Intelligent Transportation Systems* **18**.4 (2017), pp. 880–889.

[151] Jung, S.-h., Moon, B.-c. & Han, D. “Unsupervised learning for crowdsourced indoor localization in wireless networks”. *IEEE Trans. Mobile Comput.* **15**.11 (2016), pp. 2892–2906.

[152] Kai, C. et al. “Energy-efficient device-to-device communications for green smart cities”. *IEEE Transactions on Industrial Informatics* **14**.4 (2018), pp. 1542–1551.

[153] Kampanakis, P., Panburana, P., Daw, E. & Van Geest, D. “The Viability of Post-quantum X.509 Certificates.” *IACR Cryptology ePrint Archive* **2018** (2018), p. 63.

[154] Kampanakis, P. & Sikeridis, D. *Two Post-Quantum Signature Use-cases: Non-issues, Challenges and Potential Solutions*. Tech. rep. Cryptology ePrint Archive, Report 2019/1276, 2019. https://eprint.iacr.org/2019/1276.pdf, 2019.

[155] Kampanakis, P. et al. *Post-quantum public key algorithms for the Secure Shell (SSH) protocol*. Internet-Draft draft-kampanakis-curdle-pq-ssh-00. Work in Progress. Internet Engineering Task Force, 2020.

[156] Kannwischer, M. J., Rijneveld, J., Schwabe, P. & Stoffelen, K. *pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4*. Cryptology ePrint Archive, Report 2019/844. `https://eprint.iacr.org/2019/844`. 2019.

[157] Kastrinogiannis, T., Tsiropoulou, E.-E. & Papavassiliou, S. “Utility-based uplink power control in CDMA wireless networks with real-time services”. *International Conference on Ad-Hoc Networks and Wireless*. Springer. 2008, pp. 307–320.

[158] Kempener, R. & Borden, E. *Battery Storage for Renewables: Market Status and Technology Outlook*. Tech. rep. International Renewable Energy Agency, 2015.

[159] Kerrache, C. A., Lakas, A., Lagraa, N. & Barka, E. “UAV-assisted technique for the detection of malicious and selfish nodes in VANETs”. *Vehicular Communications* **11** (2018), pp. 1–11.

[160] Khatoun, R. & Zeadally, S. “Smart cities: concepts, architectures, research opportunities”. *Communications of the ACM* **59**.8 (2016), pp. 46–57.

[161] Kiesling, L. “Implications of Smart Grid Innovation for Organizational Models in Electricity Distribution”. *Smart Grid Handbook*. Ed. by Liu, C.-C., McArthur, S. & Lee, S.-J. Vol. 37. Chichester, UK: John Wiley & Sons, Ltd, 2016, pp. 1–15.

[162] Komai, K. et al. “Beacon-based multi-person activity monitoring system for day care center”. *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. IEEE. 2016, pp. 1–6.

[163] Kong, X. et al. “Mobile Crowdsourcing in Smart Cities: Technologies, Applications, and Future Challenges”. *IEEE Internet of Things Journal* **6**.5 (2019), pp. 8095–8113.

[164] Kotzias, P. et al. “Coming of age: A longitudinal study of tls deployment”. *Proceedings of the Internet Measurement Conference 2018*. ACM. 2018, pp. 415–428.

[165] Kovenock, D. & Roberson, B. “Coalitional Colonel Blotto games with application to the economics of alliances”. *Journal of Public Economic Theory* **14**.4 (2012), pp. 653–676.

[166] Kravets, R., Harris III, A. F. & Want, R. “Beacon trains: blazing a trail through dense BLE environments”. *Proceedings of the Eleventh ACM Workshop on Challenged Networks*. ACM. 2016, pp. 69–74.

[167] Krejcar, O. et al. “Smart Furniture as a Component of a Smart City—Definition based on key technologies specification”. *IEEE Access* **7** (2019), pp. 94822–94839.

[168] Kumbhar, A., Koohifar, F., Güvenç, I. & Mueller, B. “A survey on legacy and emerging technologies for public safety communications”. *IEEE Comm. Surveys & Tutorials* **19**.1 (2017), pp. 97–124.

[169] Kvaternik, K. et al. “Privacy-Preserving Platform for Transactive Energy Systems” (2017). arXiv: 1709.09597 [cs.DC].

[170] Kwiatkowski, K. *Towards Post-Quantum Cryptography in TLS*. 2019.

[171] Kwiatkowski, K. & Valenta, L. *The TLS Post-Quantum Experiment*. https://blog.cloudflare.com/the-tls-post-quantum-experiment/. 2019.

[172] Lacey, S. *New York’s Energy Czar: We Need Clean Energy Markets, Not Programs or Mandates*. https://www.greentechmedia.com/articles/read/new-york-energy-czar-we-need-clean-energy-markets-not-programs. Accessed: 2020-2-8. 2014.

[173] Lai, C. S. et al. “A review of technical standards for smart cities”. *Clean Technologies* **2**.3 (2020), pp. 290–310.

[174] Langley, A. *CECPQ1 results*. 2016.

[175] Langley, A. *CECPQ2*. 2018.

[176] Latre, S. et al. “City of things: An integrated and multi-technology testbed for IoT smart city experiments”. *2016 IEEE International Smart Cities Conference (ISC2)*. IEEE. 2016, pp. 1–8.

[177] Laufs, J., Borrion, H. & Bradford, B. “Security and the smart city: A systematic review”. *Sustainable Cities and Society* **55** (2020), p. 102023.

[178] Lawrence, D. S., La Vigne, N. G., Goff, M. & Thompson, P. S. “Lessons learned implementing gunshot detection technology: Results of a process evaluation in three major cities”. *Justice Evaluation Journal* **1**.2 (2018), pp. 109–129.

[179] Lee, J.-W., Mazumdar, R. R. & Shroff, N. B. “Joint resource allocation and base-station assignment for the downlink in CDMA networks”. *IEEE/ACM Transactions on Networking (TON)* **14**.1 (2006), pp. 1–14.

[180] Lee, K. S. “Explicit Disaster Response Features in Social Media: Safety Check and Community Help Usage on Facebook during Typhoon Mangkhut”. *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services*. 2019, pp. 1–12.

[181] Li, L., Yang, W., Alam Bhuiyan, M. Z. & Wang, G. “Unsupervised learning of indoor localization based on received signal strength”. *Wirel. Commun. Mob. Comput.* **16**.15 (2016), pp. 2225–2237.

[182] Li, Y. et al. “A Case Study of WiFi Sniffing Performance Evaluation”. *IEEE Access* **8** (2020), pp. 129224–129235.

[183] Liang, G. et al. “A review of false data injection attacks against modern power systems”. *IEEE Transactions on Smart Grid* **8**.4 (2017), pp. 1630–1638.

[184] Liu, F., Mähönen, P. & Petrova, M. “Proportional fairness-based user pairing and power allocation for non-orthogonal multiple access”. *Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE 26th Annual International Symposium on*. IEEE. 2015, pp. 1127–1131.

[185] Liu, Y., Dashti, M. & Zhang, J. “Indoor localization on mobile phone platforms using embedded inertial sensors”. *Positioning Navigation and Communication (WPNC), 2013 10th Workshop on*. IEEE. 2013, pp. 1–5.

[186] Lonvick, C. M. & Ylonen, T. *The Secure Shell (SSH) Authentication Protocol*. RFC 4252. 2006.

[187] Lonvick, C. M. & Ylonen, T. *The Secure Shell (SSH) Connection Protocol*. RFC 4254. 2006.

[188] Lonvick, C. M. & Ylonen, T. *The Secure Shell (SSH) Transport Layer Protocol*. RFC 4253. 2006.

[189] Lunness, P. “P25 radio systems training guide”. *TG-001* (2007), pp. 1–0.

[190] Marabissi, D. & Fantacci, R. “Heterogeneous Public Safety Network Architecture based on RAN slicing”. *IEEE Access* (2017).

[191] Marzal, A. & Vidal, E. “Computation of normalized edit distance and applications”. *IEEE Trans. Pattern Anal. Mach. Intell.* **15**.9 (1993), pp. 926–932.

[192] McCollough, S. W. & Henry, M. A. *Austin Energy’s Tariff Package: 2015 Cost of Service Study and Proposal to Change Base Electric Rates: Data Foundry, Inc.’s Corrected Presentation on Revenue Requirements*. 2016.

[193] Meiling, S. et al. “MONICA in hamburg: Towards large-scale iot deployments in a smart city”. *2018 European Conference on Networks and Communications (EuCNC)*. IEEE. 2018, pp. 224–9.

[194] Mendoza-Silva, G. M., Matey-Sanz, M., Torres-Sospedra, J. & Huerta, J. “BLE RSS measurements dataset for research on accurate indoor positioning”. *Data* **4**.1 (2019), p. 12.

[195] Meng, L., Kang, Q., Han, C. & Zhou, M. “Determining the Optimal Location of Terror Response Facilities Under the Risk of Disruption”. *IEEE Transactions on Intelligent Transportation Systems* **19**.2 (2018), pp. 476–486.

[196] Michael, K. & Abbas, R. “Behind COVID-19 contact trace apps: the Google–Apple partnership”. *IEEE Consumer Electronics Magazine* **9**.5 (2020), pp. 71–76.

[197] Mohammadi, M., Al-Fuqaha, A., Guizani, M. & Oh, J.-S. “Semi-supervised Deep Reinforcement Learning in Support of IoT and Smart City Services”. *IEEE Internet Things J.* (2017).

[198] Mohanty, S. P., Choppali, U. & Kougianos, E. “Everything you wanted to know about smart cities: The internet of things is the backbone”. *IEEE Consumer Electronics Magazine* **5**.3 (2016), pp. 60–70.

[199] Moriarty, K., Kaliski, B., Jonsson, J. & Rusch, A. “PKCS# 1: RSA cryptography specifications version 2.2”. *Internet Engineering Task Force, Request for Comments* **8017** (2016).

[200] Mozaffari, M., Saad, W., Bennis, M. & Debbah, M. “Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs”. *IEEE Transactions on Wireless Communications* **15**.6 (2016), pp. 3949–3963.

[201] Mozaffari, M., Saad, W., Bennis, M. & Debbah, M. “Mobile unmanned aerial vehicles (UAVs) for energy-efficient internet of things communications”. *IEEE Transactions on Wireless Communications* **16**.11 (2017), pp. 7574–7589.

[202] Mozilla. *Mozilla Telemetry Portal - Measurement Dashboard - HTTP_PAGE_TLS_-HANDSHAKE distribution for Firefox Desktop*. `https://telemetry.mozilla.org/new-pipeline/dist.html`. Beta 68/69, any OS, any architecture, any process. Web page. Accessed 2019-21-08. 2018.

[203] *MQ Telemetry Transport*. URL: `http://mqtt.org` (visited on 01/04/2016).

[204] Muraoka, K., Shikida, J. & Sugahara, H. “Feasibility of capacity enhancement of public safety LTE using device-to-device communication”. *Information and Communication Technology Convergence (ICTC), 2015 International Conference on*. IEEE. 2015, pp. 350–355.

[205] Murphy, K. P. *Machine learning: a probabilistic perspective*. The MIT press, 2012.

[206] Nam, T. & Pardo, T. A. “Smart city as urban innovation: Focusing on management, policy, and context”. *Proceedings of the 5th international conference on theory and practice of electronic governance*. ACM. 2011, pp. 185–194.

[207] Naqvi, S. A. R., Hassan, S. A., Pervaiz, H. & Ni, Q. “Drone-Aided Communication as a Key Enabler for 5G and Resilient Public Safety Networks”. *IEEE Comm. Mag.* **56**.1 (2018), pp. 36–42.

[208] Narendra, K. S. & Thathachar, M. A. “Learning automata-a survey”. *IEEE Transactions on systems, man, and cybernetics* 4 (1974), pp. 323–334.

[209] Naylor, D. et al. “The cost of the S in HTTPS”. *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*. ACM. 2014, pp. 133–140.

[210] Nejatollahi, H. et al. “Post-Quantum Lattice-Based Cryptography Implementations: A Survey”. *ACM Comput. Surv.* **51**.6 (2019).

[211] NERC. *State of Reliability 2018 - nerc.com*. 2018.

[212] NERC Steering Group et al. “Technical analysis of the August 14, 2003, blackout: What happened, why, and what did we learn”. *report to the NERC Board of Trustees* (2004).

[213] Newcomb, J., Lacy, V. & Hansen, L. *New Business Models for the Distribution Edge*. Tech. rep. Rocky Mountain Institute, 2013.

[214] Ng, P. C., Spachos, P., Gregori, S. & Plataniotis, K. “Epidemic Exposure Notification with Smartwatch: A Proximity-Based Privacy-Preserving Approach”. *arXiv preprint arXiv:2007.04399* (2020).

[215] Ng, P. C., Spachos, P. & Plataniotis, K. “COVID-19 and Your Smartphone: BLE-based Smart Contact Tracing”. *arXiv preprint arXiv:2005.13754* (2020).

[216] NIST. *Post-Quantum Cryptography Round 2 Submissions*. `https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions`. 2020.

[217] Pan, J. J. et al. “Tracking mobile users in wireless networks via semi-supervised colocalization”. *IEEE Trans. Pattern Anal. Mach. Intell.* **34**.3 (2012), pp. 587–600.

[218] Pang, Y. et al. “Spath: Finding the safest walking path in smart cities”. *IEEE Transactions on Vehicular Technology* **68**.7 (2019), pp. 7071–7079.

[219] Paquin, C., Stebila, D. & Tamvada, G. “Benchmarking post-quantum cryptography in tls”. *International Conference on Post-Quantum Cryptography*. Springer. 2020, pp. 72–91.

[220] Park, J., Lee, H., Eom, S. & Lee, I. “Minimum Throughput Maximization in UAV-Aided Wireless Powered Communication Networks”. *arXiv preprint arXiv:1801.02781* (2018).

[221] Perea, A. et al. *U.S. Solar Market Insight*. Tech. rep. Wood Mackenzie Power & Renewables; Solar Energy Industries Association, 2019.

[222] Perry, T. S. “San Diego’s streetlights get smart”. *IEEE Spectrum* **55**.1 (2018), pp. 30–31.

[223] Petropoulos, A. & Antonakopoulos, T. “Indoor Location Estimation using a Pair of Wearable Devices”. *IEICE Information and Communication Technology Forum (ICTF)*. IEICE. 2016.

[224] Petropoulos, A., Sikeridis, D. & Antonakopoulos, T. “SPoMo: IMU-based real-time sitting posture monitoring”. *2017 IEEE 7th International Conference on Consumer Electronics-Berlin (ICCE-Berlin)*. IEEE. 2017, pp. 5–9.

[225] Petropoulos, A., Sikeridis, D. & Antonakopoulos, T. “Wearable smart health advisors: An IMU-enabled posture monitor”. *IEEE Consumer Electronics Magazine* **9**.5 (2020), pp. 20–27.

[226] Pettit, C. et al. “Planning support systems for smart cities”. *City, culture and society* **12** (2018), pp. 13–24.

[227] Prasad, A. et al. “Enabling group communication for public safety in LTE-Advanced networks”. *Journal of Network and Computer Applications* **62** (2016), pp. 41–52.

[228] Project, O. *liboqs*. `https://github.com/open-quantum-safe/liboqs`. Web page. Accessed 2020-02-06. 2020.

[229] Project, O. *OQS OpenSSH*. `https://github.com/open-quantum-safe/openssh`. Web page. Accessed 2020-02-06. 2020.

[230] Project, O. *OQS OpenSSL*. `https://github.com/open-quantum-safe/openssl`. Web page. Accessed 2020-02-06. 2020.

[231] Project, P. *PQClean*. `https://github.com/PQClean/PQClean`. Web page. Accessed 2019-02-09. 2019.

[232] Qiu, T. et al. “How Can Heterogeneous Internet of Things Build our Future: A Survey”. *IEEE Communications Surveys Tutorials* **PP**.99 (2018), pp. 1–1.

[233] Qiu, T. et al. “How Can Heterogeneous Internet of Things Build our Future: A Survey”. *IEEE Communications Surveys Tutorials* **PP**.99 (2018), pp. 1–1.

[234] Quasim, M. T., Khan, M. A., Algarni, F. & Alshahrani, M. M. “Fundamentals of Smart Cities”. *Smart Cities: A Data Analytics Perspective*. Springer, 2021, pp. 3–16.

[235] Rai, A., Chintalapudi, K. K., Padmanabhan, V. N. & Sen, R. “Zee: Zero-effort crowdsourcing for indoor localization”. *Proc., ACM MobiCom*. 2012, pp. 293–304.

[236] Ranadheera, S., Maghsudi, S. & Hossain, E. “Minority games with applications to distributed decision making and control in wireless networks”. *IEEE Wireless Comm.* **24**.5 (2017), pp. 184–192.

[237] Rao, N. S. et al. “Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models”. *Risk Analysis* **36**.4 (2016), pp. 694–710.

[238] Razaghpanah, A. et al. “Studying TLS usage in Android apps”. *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*. 2017, pp. 350–362.

[239] Rescorla, E. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. 2018.

[240] Rescorla, E., Barnes, R. & Tschofenig, H. *Compact TLS 1.3*. Internet-Draft draft-rescorla-tls-ctls-04. Work in Progress. Internet Engineering Task Force, 2020. 17 pp.

[241] Reuter, C. & Kaufhold, M.-A. “Fifteen years of social media in emergencies: a retrospective review and future directions for crisis informatics”. *Journal of Contingencies and Crisis Management* **26**.1 (2018), pp. 41–57.

[242] Reuter, C., Pätsch, K. & Runft, E. “IT for Peace? Fighting Against Terrorism in Social Media–An Explorative Twitter Study”. *i-com* **16**.2 (2017), pp. 181–193.

[243] Roberson, B. “The colonel blotto game”. *Economic Theory* **29**.1 (2006), pp. 1–24.

[244] Roberson, B. & Kvasov, D. “The non-constant-sum Colonel Blotto game”. *Economic Theory* **51**.2 (2012), pp. 397–433.

[245] Roberts, D. *Rooftop solar is just the beginning; utilities must innovate or go extinct*. `https://grist.org/climate-energy/rooftop-solar-is-just-the-beginning-utilities-must-innovate-or-go-extinct/`. Accessed: 2020-2-8. 2014.

[246] Roberts, D. *New York’s revolutionary plan to remake its power utilities*. `https://www.vox.com/2015/10/5/9453131/new-york-utilities-rev`. Accessed: 2020-2-8. 2015.

[247] Roy, A., Kamhoua, C. A. & Mohapatra, P. “Game Theoretic Characterization of Collusive Behavior Among Attackers”. *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. 2018, pp. 2078–2086.

[248] Rüth, J., Bormann, C. & Hohlfeld, O. “Large-scale scanning of TCP’s initial window”. *Proceedings of the 2017 Internet Measurement Conference*. 2017, pp. 304–310.

[249] Rüth, J. & Hohlfeld, O. “Demystifying TCP initial window configurations of content distribution networks”. *2018 Network Traffic Measurement and Analysis Conference (TMA)*. IEEE. 2018, pp. 1–8.

[250] Saarinen, M.-J. O. “Mobile energy requirements of the upcoming NIST post-quantum cryptography standards”. *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. IEEE. 2020, pp. 23–30.

[251] Sandler, T. “Terrorism & game theory”. *Simulation & Gaming* **34**.3 (2003), pp. 319–337.

[252] Sansano-Sansano, E., Aranda, F. J., Montoliu, R. & Álvarez, F. J. “BLE-GSpeed: A New BLE-Based Dataset to Estimate User Gait Speed”. *Data* **5**.4 (2020), p. 115.

[253] Saraydar, C. U., Mandayam, N. B. & Goodman, D. J. “Efficient power control via pricing in wireless data networks”. *IEEE transactions on Communications* **50**.2 (2002), pp. 291–303.

[254] Sarkar, T. K. et al. “A survey of various propagation models for mobile communication”. *IEEE Antennas Propag. Mag.* **45**.3 (2003), pp. 51–82.

[255] Shah, S. A. et al. “Towards Disaster Resilient Smart Cities: Can Internet of Things and Big Data Analytics Be the Game Changers?” *IEEE Access* **7** (2019), pp. 91885–91903.

[256] Sharma, V. et al. “Intelligent deployment of UAVs in 5G heterogeneous communication environment for improved coverage”. *Journal of Network and Computer Applications* **85** (2017), pp. 94–105.

[257] SHODAN. *HTTPS (443) Overview*. `https://www.shodan.io/report/nWlAWhKG`. 2019.

[258] Shor, P. W. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. *SIAM J. on Computing* **26**.5 (1997), pp. 1484–1509.

[259] ShotSpotter. *ShotSpotter FAQ. Newark, CA: ShotSpotter, Inc.* `www.shotspotter.com/wp-content/uploads/2018/08/FAQ_Aug_2018.pdf`.

[260] Sikeridis, D., Rimal, B. P., Papapanagiotou, I. & Devetsikiotis, M. “Unsupervised Crowd-Assisted Learning Enabling Location-Aware Facilities”. *IEEE Internet of Things Journal* (2018), pp. 1–1.

[261] Sikeridis, D. “IoT-enabled Knowledge Extraction and Edge Device Sustainability in Smart Cities”. *2020 IEEE International Conference on Smart Computing (SMARTCOMP)*. 2020, pp. 264–265.

[262] Sikeridis, D., Bidram, A., Devetsikiotis, M. & Reno, M. J. “A blockchain-based mechanism for secure data exchange in smart grid protection systems”. *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE. 2020, pp. 1–6.

[263] Sikeridis, D. & Devetsikiotis, M. “Joint Capacity Modeling for Electric Vehicles in V2I-enabled Wireless Charging Highways”. *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE. 2020, pp. 1–6.

[264] Sikeridis, D., Devetsikiotis, M. & Papapanagiotou, I. “A Cloud-Assisted Infrastructure for Occupancy Tracking in Smart Facilities”. *IBM Cloud Academy Conference (ICA CON)*. 2017.

[265] Sikeridis, D., Devetsikiotis, M. & Papapanagiotou, I. “Occupant Tracking in Smart Facilities: An Experimental Study”. *Signal and Information Processing (GlobalSIP), 2017 IEEE Global Conference on*. IEEE. 2017.

[266] Sikeridis, D., EleniTsiropoulou, E., Devetsikiotis, M. & Papavassiliou, S. “Self-adaptive energy efficient operation in UAV-assisted public safety networks”. *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE. 2018, pp. 1–5.

[267] Sikeridis, D., Kampanakis, P. & Devetsikiotis, M. “Assessing the Overhead of Post-Quantum Cryptography in TLS 1.3 and SSH”. *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*. New York, NY, USA: Association for Computing Machinery, 2020, 149–156.

[268] Sikeridis, D., Kampanakis, P. & Devetsikiotis, M. “Post-Quantum Authentication in TLS 1.3: A Performance Study”. *Network and Distributed Systems Security (NDSS) Symposium 2020 23-26 February 2020, San Diego, CA, USA*. The Internet Society, 2020.

[269] Sikeridis, D., Papapanagiotou, I. & Devetsikiotis, M. “BLEBeacon: A Real-Subject Trial Dataset from Mobile Bluetooth Low Energy Beacons”. *arXiv preprint arXiv:1802.08782* (2018).

[270] Sikeridis, D., Papapanagiotou, I. & Devetsikiotis, M. *CRAWDAD dataset unm/blebeacon (v. 2019-03-12)*. 2019.

[271] Sikeridis, D., Papapanagiotou, I., Rimal, B. P. & Devetsikiotis, M. “A Comparative taxonomy and survey of public cloud infrastructure vendors”. *arXiv preprint arXiv:1710.01476* (2017).

[272] Sikeridis, D., Rimal, B. P., Papapanagiotou, I. & Devetsikiotis, M. “Unsupervised crowd-assisted learning enabling location-aware facilities”. *IEEE Internet of Things Journal* **5**.6 (2018), pp. 4699–4713.

[273] Sikeridis, D., Tsiropoulou, E. E., Devetsikiotis, M. & Papavassiliou, S. “Context-aware wireless-protocol selection in heterogeneous public safety networks”. *IEEE Transactions on Vehicular Technology* **68**.2 (2018), pp. 2009–2013.

[274] Sikeridis, D., Tsiropoulou, E. E., Devetsikiotis, M. & Papavassiliou, S. “Energy-efficient orchestration in wireless powered Internet of Things infrastructures”. *IEEE Transactions on Green Communications and Networking* **3**.2 (2018), pp. 317–328.

[275] Sikeridis, D., Tsiropoulou, E. E., Devetsikiotis, M. & Papavassiliou, S. “Socio-physical Energy-Efficient Operation in the Internet of Multipurpose Things”. *Communications (ICC), 2018 IEEE International Conference on*. IEEE. 2018.

[276] Sikeridis, D., Tsiropoulou, E. E., Devetsikiotis, M. & Papavassiliou, S. “Socio-spatial resource management in wireless powered public safety networks”. *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE. 2018, pp. 810–815.

[277] Sikeridis, D., Tsiropoulou, E. E., Devetsikiotis, M. & Papavassiliou, S. “Wireless powered Public Safety IoT: A UAV-assisted adaptive-learning approach towards energy efficiency”. *Journal of Network and Computer Applications* (2018).

[278] Singer, N. “Mission control, built for cities: IBM takes "smarter cities" concept to Rio de Janeiro”. *New York Times* **3** (2012). accessed on April 10 2020.

[279] Singh, V. K., Ozen, A. & Govindarasu, M. “Stealthy cyber attacks and impact analysis on wide-area protection of smart grid”. *2016 North American Power Symposium (NAPS)*. IEEE. 2016, pp. 1–6.

[280] Sivrikaya, F. et al. “Internet of Smart City Objects: A Distributed Framework for Service Discovery and Composition”. *IEEE Access* **7** (2019), pp. 14434–14454.

[281] *Smart Cities Market Analysis Report By Application (Governance, Buildings, Utilities, Transportation, Healthcare, Environmental Solution), By Region, And Segment Forecasts, 2019 - 2025*. `https://www.researchandmarkets.com/r/ae3abx`. 2019.

[282] Sokolova, M. & Lapalme, G. “A systematic analysis of performance measures for classification tasks”. *Information Processing & Management* **45**.4 (2009), pp. 427–437.

[283] Somasundaram, S et al. *Reference Guide for a Transaction-Based Building Controls Framework*. Tech. rep. Pacific Northwest National Laboratory, 2014.

[284] Sorour, S., Lostanlen, Y., Valaee, S. & Majeed, K. “Joint indoor localization and radio map construction with limited deployment load”. *IEEE Trans. Mobile Comput.* **14**.5 (2015), pp. 1031–1043.

[285] Sotres, P. et al. “Practical lessons from the deployment and management of a smart city Internet-of-Things infrastructure: The smartsantander testbed case”. *IEEE Access* **5** (2017), pp. 14309–14322.

[286] Späth, P. & Knieling, J. “How EU-funded smart city experiments influence modes of planning for mobility: Observations from Hamburg”. *Urban Transformations* **2**.1 (2020), pp. 1–17.

[287] St. John, J. *An Inside Look at a Groundbreaking Solar-Storage Procurement in California*. https://www.greentechmedia.com/articles/read/inside-california-community-energy-providers-groundbreaking-solar-storage-p. Accessed: 2020-1-19. 2019.

[288] St. John, J. *US Storage Market Rebounds as Outage-Scarred California Promises Big 2020 Growth*. https://www.greentechmedia.com/articles/read/us-storage-market-rebounds-in-q3-as-calif-power-outages-loom-large. Accessed: 2020-1-19. 2019.

[289] Standards, N. I. of & Technology. *Specification for the Secure Hash Standard. Federal Information Professing Standards (FIPS) 180-2*. https://csrc.nist.gov/CSRC/media/Publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf. 2002.

[290] Starbird, K. et al. “Rumors, false flags, and digital vigilantes: Misinformation on twitter after the 2013 boston marathon bombing”. *iConference 2014 Proceedings* (2014).

[291] *State of the Electric Utility 2015 - Survey Results*. Tech. rep. Utility Dive, 2015.

[292] Stebila, D. & Mosca, M. *Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project*. Cryptology ePrint Archive, Report 2016/1017. https://eprint.iacr.org/2016/1017. 2016.

[293] Steblia, D., Fluhrer, S. & Gueron, S. *Design issues for hybrid key exchange in TLS 1.3*. Internet-Draft draft-stebila-tls-hybrid-design-01. Work in Progress. Internet Engineering Task Force, 2019. 32 pp.

[294] Steblia, D., Fluhrer, S. & Gueron, S. *Design issues for hybrid key exchange in TLS 1.3*. Internet-Draft draft-stebila-tls-hybrid-design-01. Work in Progress. Internet Engineering Task Force, 2019. 32 pp.

[295] Stellios, I. et al. “A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services”. *IEEE Communications Surveys & Tutorials* **20**.4 (2018), pp. 3453–3495.

[296] Stieglitz, S., Bunker, D., Mirbabaie, M. & Ehnis, C. “Sense-making in social media during extreme events”. *Journal of Contingencies and Crisis Management* **26**.1 (2018), pp. 4–15.

[297] Strickland, E. “Cisco bets on South Korean smart city”. *IEEE Spectrum* **48**.8 (2011), pp. 11–12.

[298] Sullivan, N. “ECDSA: The digital signature algorithm of a better internet”. *CloudFlare* (2014).

[299] Swain, V. D. et al. “Leveraging wifi network logs to infer social interactions: A case study of academic performance and student behavior”. *arXiv preprint arXiv:2005.11228* (2020).

[300] Team, P.-P. *Pan-European Privacy-Preserving Proximity Tracing*. 2020.

[301] *The MONICA project, Management Of Networked IoT Wearables – Very Large Scale Demonstration of Cultural Societal Applications*. `https://www.monica-project.eu`.

[302] Things Case Study, G. I. of. *CritiCal CommuniCations IoT - Concepts Paper*. `https://www.gsma.com/iot/wp-content/uploads/2019/12/202001_GSMA_IoT_Critical-Comms-IoT-Concepts-Paper.pdf`.

[303] Thomas, C. D. *N-Dimensional Blotto Game with Asymmetric Battlefield Values*. Department of Economics Working Papers 130116. The University of Texas at Austin, Department of Economics, 2009.

[304] Thomson, M. *Suppressing Intermediate Certificates in TLS*. Internet-Draft draft-thomson-tls-sic-00. Work in Progress. Internet Engineering Task Force, 2019. 4 pp.

[305] Tonetto, L., Untersperger, M. & Ott, J. “Towards Exploiting Wi-Fi Signals From Low Density Infrastructure for Crowd Estimation”. *Proceedings of the 14th Workshop on Challenged Networks*. 2019, pp. 27–32.

[306] *Transactive Energy Application Landscape Scenarios*. Tech. rep. SGIP, 2016.

[307] Tsiropoulou, E. E., Katsinis, G. K. & Papavassiliou, S. “Distributed uplink power control in multiservice wireless networks via a game theoretic approach with convex pricing”. *IEEE Transactions on Parallel and Distributed Systems* **23**.1 (2012), pp. 61–68.

[308] Tuna, G., Nefzi, B. & Conte, G. “Unmanned aerial vehicle-aided communications system for disaster recovery”. *Journal of Network and Computer Applications* **41** (2014), pp. 27–36.

[309] Tweed, K. *New York Launches Major Regulatory Reform for Utilities*. `https://www.greentechmedia.com/articles/read/new-york-launches-major-regulatory-reform-for-utilities`. Accessed: 2020-2-8. 2014.

[310] *United Nations Sustainable Development Goals (SDGs)*. `https://sustainabledevelopment.un.org`. 2019.

[311] *U.S. Energy Storage Monitor Q4 2019*. Tech. rep. Wood Mackenzie Power & Renewables; ESA U.S. Energy Storage Monitor, 2019.

[312] Valenta, L., Sullivan, N., Sanso, A. & Heninger, N. “In search of CurveSwap: Measuring elliptic curve implementations in the wild”. *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. 2018, pp. 384–398.

[313] Venkataramanan, V et al. “Enhancing Microgrid Resiliency Against Cyber Vulnerabilities”. *2018 IEEE Industry Applications Society Annual Meeting (IAS)*. IEEE. 2018, pp. 1–8.

[314] Vu, D. Q., Loiseau, P. & Silva, A. “Efficient Computation of Approximate Equilibria in Discrete Colonel Blotto Games”. *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, IJCAI-18*. International Joint Conferences on Artificial Intelligence Organization, 2018, pp. 519–526.

[315] Wan, S., Lu, J., Fan, P. & Letaief, K. B. “To smart city: Public safety network design for emergency”. *IEEE access* **6** (2017), pp. 1451–1460.

[316] Wang, B., Chen, Q., Yang, L. T. & Chao, H.-C. “Indoor smartphone localization via fingerprint crowdsourcing: Challenges and approaches”. *IEEE Wireless Communications* **23**.3 (2016), pp. 82–89.

[317] Wang, H. et al. “Resource Allocation for Energy Harvesting-Powered D2D Communication Underlaying UAV-Assisted Networks”. *IEEE Transactions on Green Communications and Networking* **2**.1 (2018), pp. 14–24.

[318] Wang, P., Angarita, R. & Renna, I. “Is this the Era of Misinformation yet? Combining Social Bots and Fake News to Deceive the Masses”. *The 2018 Web Conference Companion*. 2018.

[319] Wang, W. et al. “A survey on consensus mechanisms and mining management in blockchain networks”. *arXiv preprint arXiv:1805.02707* (2018).

[320] Wang, X., Gao, L., Mao, S. & Pandey, S. “CSI-based fingerprinting for indoor localization: A deep learning approach”. *IEEE Transactions on Vehicular Technology* **66**.1 (2017), pp. 763–776.

[321] Welsh, D. & Roy, N. “Smartphone-based mobile gunshot detection”. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE. 2017, pp. 244–249.

[322] Wen, Y., Tian, X., Wang, X. & Lu, S. “Fundamental limits of RSS fingerprinting based indoor localization”. *Proc., IEEE INFOCOM*. 2015, pp. 2479–2487.

[323] Westgarth, A. *Turning on Project Loon in Puerto Rico*. `https://blog.x.company/turning-on-project-loon-in-puerto-rico-f3aa41ad2d7f`. accessed on Mar. 22, 2018. 2017.

[324] Woetzel, J. et al. “Smart cities: Digital solutions for a more livable future”. *McKinsey Global Institute: New York, NY, USA* (2018), pp. 1–152.

[325] Wu, C., Yang, Z. & Liu, Y. “Smartphones based crowdsourcing for indoor localization”. *IEEE Trans. Mobile Comput.* **14**.2 (2015), pp. 444–457.

[326] Wu, C., Yang, Z., Liu, Y. & Xi, W. “WILL: Wireless indoor localization without site survey”. *IEEE Transactions on Parallel and Distributed Systems* **24**.4 (2013), pp. 839–848.

[327] Xie, L., Xu, J. & Zhang, R. “Throughput Maximization for UAV-Enabled Wireless Powered Communication Networks”. *arXiv preprint arXiv:1801.04545* (2018).

[328] Xu, L. & Jordan, M. I. “On convergence properties of the EM algorithm for Gaussian mixtures”. *Neural computation* **8**.1 (1996), pp. 129–151.

[329] Xu, Z. et al. “Social Sensors Based Online Attention Computing of Public Safety Events”. *IEEE Transactions on Emerging Topics in Computing* **5**.3 (2017), pp. 403–411.

[330] Yang, Z. et al. “Energy Efficient Resource Allocation in Machine-to-Machine Communications With Multiple Access and Energy Harvesting for IoT”. *IEEE Internet of Things Journal* **5**.1 (2018), pp. 229–245.

[331] Yaqoob, I. et al. “Enabling communication technologies for smart cities”. *IEEE Communications Magazine* **55**.1 (2017), pp. 112–120.

[332] Yee, P. E. *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 6818. 2013.

[333] Yujian, L. & Bo, L. “A normalized Levenshtein distance metric”. *IEEE Trans. Pattern Anal. Mach. Intell.* **29**.6 (2007), pp. 1091–1095.

[334] Zafari, F. & Papapanagiotou, I. “Enhancing iBeacon Based Micro-Location with Particle Filtering”. *2015 IEEE Global Communications Conference (GLOBECOM)*. 2015, pp. 1–7.

[335] Zafari, F., Papapanagiotou, I. & Christidis, K. “Microlocation for Internet-of-Things-Equipped Smart Buildings”. *IEEE Internet of Things Journal* **3**.1 (2016), pp. 96–112.

[336] Zafari, F., Papapanagiotou, I., Devetsikiotis, M. & Hacker, T. “An iBeacon based Proximity and Indoor Localization System”. *arXiv preprint arXiv:1703.07876* (2017).

[337] Zafari, F., Papapanagiotou, I., Devetsikiotis, M. & Hacker, T. J. “Enhancing the Accuracy of iBeacons for Indoor Proximity-based Services”. *IEEE ICC 2017*. IEEE. 2017.

[338] Zhang, D. et al. “On Scalable and Robust Truth Discovery in Big Data Social Media Sensing Applications”. *IEEE Transactions on Big Data* **5**.2 (2019), pp. 195–208.

[339] Zhang, Q., Fu, B., Feng, Z. & Li, W. “Utility-Maximized Two-Level Game-Theoretic Approach for Bandwidth Allocation in Heterogeneous Radio Access Networks”. *IEEE Transactions on Vehicular Technology* **66**.1 (2017), pp. 844–854.

[340] Zhang, R., Hoflinger, F. & Reindl, L. “Inertial sensor based indoor localization and monitoring system for emergency responders”. *IEEE Sensors Journal* **13**.2 (2013), pp. 838–848.

[341] Zhou, X. et al. “Human mobility patterns in cellular networks”. *IEEE communications letters* **17**.10 (2013), pp. 1877–1880.

[342] Zhou, Y. et al. “Understanding Crowd Behaviors in a Social Event by Passive WiFi Sensing and Data Mining”. *IEEE Internet of Things Journal* **7**.5 (2020), pp. 4442–4454.

[343] Zhu, J. et al. “IBM cloud computing powering a smarter planet”. *IEEE International Conference on Cloud Computing*. Springer. 2009, pp. 621–625.

Appendices

Appendix A

Proofs of Chapter 6 Theorems

A.1 Proof of Theorem 4

The expected Nash equilibrium payoff functions of three SCDG players after stage three are given by Eq. 6.11 depending on the ratio of available player budgets. The TO during the second stage reacts to the budget allocation of the SC entities ($r^{1\to 2}$, $r^{2\to 1}$) and allocates his budget τ in an effort to maximize his expected payoff. For our simplified case where $\frac{2}{|\Theta_1|} < \frac{\tau}{d_1} < 1$ and $\frac{2}{|\Theta_2|} < \frac{\tau}{d_2} < 1$ the expected payoff of T as a function of his own budget allocation across the physical (τ_1) and social (τ_2) battles is:

$$\Psi^T(\tau_1) = \phi_1 \cdot \frac{\tau_1}{2d_1} + \phi_2 \cdot \frac{\tau_2}{2d_2} \Leftrightarrow \Psi^T = \phi_1 \frac{\tau_1}{2d_1} + \phi_2 \frac{\tau - \tau_1}{2d_2}$$

The first derivative is $\frac{\partial \Psi^T}{\partial \tau_1} = \frac{\phi_1}{2d_1} - \frac{\phi_2}{2d_2}$ and we have to consider three distinct cases:

1. $\frac{\partial \Psi^T}{\partial \tau_1} = 0 \Leftrightarrow \frac{\phi_1}{2d_1} = \frac{\phi_2}{2d_2}$, thus any budget allocation $\tau_1 \in [0, \tau]$ is optimal for the TO
2. $\frac{\partial \Psi^T}{\partial \tau_1} > 0 \Leftrightarrow \frac{\phi_1}{2d_1} > \frac{\phi_2}{2d_2}$, then Ψ^T is increasing in $\tau_1 \in [0, \tau]$ and will be maximum at $\Psi^T(\tau_1 = \tau) = \frac{\phi_1 \tau}{2d_1}$ which means that the TO will allocate all the budget fighting the physical SC game (CBG 1)
3. $\frac{\partial \Psi^T}{\partial \tau_1} < 0 \Leftrightarrow \frac{\phi_1}{2d_1} < \frac{\phi_2}{2d_2}$, then followig the logic of case b the TO allocates all his budget to the social game (CBG 2)

Therefore:

$$\tau_1^* = T^*(r^{1\to2}, r^{2\to1}) = \begin{cases} any\ choice \in [0,\tau], & if\ \ \frac{\phi_1}{d_1} = \frac{\phi_2}{d_2} \\ \tau, & if\ \ \frac{\phi_1}{d_1} > \frac{\phi_2}{d_2} \\ 0, & if\ \ \frac{\phi_1}{d_1} < \frac{\phi_2}{d_2} \end{cases}$$

$$\tau_2^* = \tau - \tau_1^* \tag{A.1}$$

We will now focus on the first SCDG stage, where the two SC entities should decide on the budget transfer between them. In this stage the known SCDG parameters are the two CBGs' values (ϕ_1, ϕ_2) and each SC entity's emergency response budget c_1, c_2. Assume $\frac{\phi_1}{c_1} < \frac{\phi_2}{c_2}$. In this case if no budget transfer is performed during stage 1 the TO will allocate all his budget to the social game 2 ($\tau_1^* = 0, \tau_2^* = \tau$) according to the aforementioned second stage response. A positive transfer from player two (ICT) to player one (ESA) will reduce the payoff of player two and will make no impact to the payoff of player one. Thus, $r^{2\to1} = 0$ for $\frac{\phi_1}{c_1} < \frac{\phi_2}{c_2}$. Let us now assume that a positive transfer will occur from the ESA to the ICT agency while maintaining the conditions that will trigger the same TO response in stage two[1], namely $\frac{2}{|\Theta_1|} < \frac{\tau}{c_1 - r^{1\to2}} < 1$, $\frac{2}{|\Theta_2|} < \frac{\tau}{c_2 + r^{1\to2}} < 1$, and $\frac{\phi_1}{c_1 - r^{1\to2}} < \frac{\phi_2}{c_2 + r^{1\to2}}$. Then we can calculate the maximum budget transfer that improves the payoff of player two and maintains the payoff of player one (pareto improving transfer [165]) as:

$$\frac{\phi_1}{c_1 - r^{1\to2}} < \frac{\phi_2}{c_2 + r^{1\to2}} \Leftrightarrow r^{1\to2} < \frac{\phi_2 c_1 - \phi_1 c_2}{\phi_1 + \phi_2} \tag{A.2}$$

The ESA (player 1) will never transfer budget that exceeds $\frac{\phi_2 c_1 - \phi_1 c_2}{\phi_1 + \phi_2}$ since it would lead to a different TO response that would reduce his payoff. Since the TO assigns all his budget to fight the social CBG, the ESA (acting according to the SPNE) is allowed to transfer up to $\frac{\phi_2 c_1 - \phi_1 c_2}{\phi_1 + \phi_2}$ in order to maintain this response and aid the ICT agency. The analysis is analogous for the $\frac{\phi_1}{c_1} < \frac{\phi_2}{c_2}$ case. Finally when $\frac{\phi_1}{c_1} = \frac{\phi_2}{c_2}$ no transfer guarantees an improvement for the SC entities' payoff thus no budget exchange is performed. □

[1]This requirement stems from the one-stage deviation principle, Section 6.3 - Theorem 3

A.2 Proof of Theorem 5

For the specific parameters of this case ($d_1+d_2<\tau$, and $\frac{\tau_1}{d_1}<1$, $\frac{\tau_2}{d_2}<1$) the expected payoff of T as a function of his own budget allocation across the physical (τ_1) and social (τ_2) battles following Eq. 6.11 is:

$$\begin{aligned}\Psi^T(\tau_1)&=\phi_1-\phi_1\frac{d_1}{2\tau_1}+\phi_2-\phi_2\cdot\frac{d_2}{2\tau_2}\overset{\tau_2=\tau-\tau_1}{\Longleftrightarrow}\\ \Psi^T(\tau_1)&=\phi_1-\phi_1\frac{d_1}{2\tau_1}+\phi_2-\phi_2\cdot\frac{d_2}{2(\tau-\tau_1)}\end{aligned}\tag{A.3}$$

The first derivative is:

$$\frac{\partial\Psi^T(\tau_1)}{\partial\tau_1}=\frac{\phi_1 d_1}{2(\tau_1)^2}-\frac{\phi_2 d_2}{2(\tau-\tau_1)^2}\tag{A.4}$$

The budget allocation to CBG_1 that will maximize the TO's payoff is:

$$\frac{\partial\Psi^T(\tau_1)}{\partial\tau_1}=0\Leftrightarrow\frac{(\tau-\tau_1)^2}{(\tau_1)^2}=\frac{\phi_2 d_2}{\phi_1 d_1}\Leftrightarrow\frac{\tau-\tau_1}{\tau_1}=\sqrt{\frac{\phi_2 d_2}{\phi_1 d_1}}$$

since $\tau-\tau_1$ is a strictly positive quantity. Thus, $\tau_1^*=\frac{\tau}{1+\sqrt{\frac{\phi_2 d_2}{\phi_1 d_1}}}$. Also, since $\frac{\partial^2\Psi^T(\tau_1)}{\partial\tau_1^2}=-\frac{\phi_1 d_1\tau_1}{(\tau_1)^4}-\frac{\phi_2 d_2(\tau-\tau_1)}{(\tau-\tau_1)^4}<0$ as $\tau-\tau_1>0$, $\Psi^T(\tau_1)$ is concave and τ_1^* a maximum. Given that, without loss of generality we assume that the ESA (player 1) transfers positive budget equal to r, $r\geq 0$ to the ICT agency (player 2), while their initial budget is c_1, c_2 respectively. Then the ESA payoff (Eq. 6.11) is:

$$\Psi^1(r)=\phi_1\frac{c_1-r}{2\tau_1^*(r)}=\phi_1\frac{c_1-r}{2\cdot\frac{\tau}{1+\sqrt{\frac{\phi_2(c_2+r)}{\phi_1(c_1-r)}}}}\tag{A.5}$$

Finding the first and second derivative yields:

$$\frac{\partial\Psi^1(r)}{\partial r}=-\frac{\phi_1}{2\tau}+\frac{\sqrt{\phi_1\phi_2}}{4\tau}\cdot\frac{c_1-c_2-2r}{\sqrt{c_1-r}\cdot\sqrt{c_2+r}}$$

and

$$\frac{\partial^2\Psi^1(r)}{\partial r^2}=-\frac{\sqrt{\phi_1\phi_2}(c_2+c_1)^2}{8\tau(c_1-r)^{\frac{3}{2}}(c_2+r)^{\frac{3}{2}}}$$

Since $\frac{\partial^2\Psi^1(r)}{\partial r^2} < 0$, $\Psi^1(r)$ is concave. Evidently, it is beneficial for the ESA to transfer to the ICT agency iff at the beginning of the domain of definition:

$$\left.\frac{\partial\Psi^1(r)}{\partial r}\right|_{r=0} > 0 \Leftrightarrow -\frac{\phi_1}{2\tau} + \frac{\sqrt{\phi_1\phi_2}}{4\tau}\cdot\frac{c_1-c_2-2r}{\sqrt{c_1-r}\cdot\sqrt{c_2+r}} > 0$$
$$\Leftrightarrow \frac{c_1-c_2}{2\sqrt{c_1c_2}} > \sqrt{\frac{\phi_1}{\phi_2}}$$

This is a necessary condition for the existence of a budget transfer from player 1 to player 2 that is mutually beneficial. The condition also implies that $c_1 - c_2 > 2\sqrt{\frac{\phi_1}{\phi_2}}\sqrt{c_1c_2} > 0 \Leftrightarrow c_1 > c_2$. Regarding the optimal amount of budget to be transferred $r^{*1\to2}$, it is given by:

$$\frac{\partial\Psi^1(r)}{\partial r} = 0 \Leftrightarrow \ldots \Leftrightarrow$$
$$r^2 - (c_1-c_2)r + \frac{1}{4}\frac{\phi_2(c_1-c_2)^2}{\phi_1+\phi_2} - \frac{\phi_1}{\phi_1+\phi_2}c_1c_2 \Leftrightarrow \ldots \Leftrightarrow$$
$$r = \frac{c_1-c_2}{2} \pm \frac{c_1+c_2}{2}\sqrt{\frac{\phi_1}{\phi_1+\phi_2}}$$

Since r describes a transfer from player 1 to player 2 there is the extra restriction of $r < c_1$. Thus, the only viable solution is $r^{*1\to2} = \frac{c_1-c_2}{2} - \frac{c_1+c_2}{2}\sqrt{\frac{\phi_1}{\phi_1+\phi_2}}$.

Regarding the opposite transfer ($r^{*2\to1}$) if we assume that a quantity r is transferred from the ICT agency (player 2) to the ESA then the payoff of player 2 is given by:

$$\Psi^2(r) = \frac{\phi_2}{2}\frac{c_2-r}{\tau_2^*(r)} = \frac{\phi_2}{2}\frac{c_2-r}{\tau-\tau_1^*(r)} = \ldots =$$
$$\frac{\sqrt{\phi_1\phi_2}}{2\tau}(\sqrt{(c_2-r)(c_1+r)}) + \frac{\phi_2}{2\tau}(c_2-r) \tag{A.6}$$

The first derivative:

$$\frac{\partial\Psi^2(r)}{\partial r} = \ldots = -(\frac{\sqrt{\phi_1\phi_2}}{4\tau}\cdot\frac{c_1-c_2+2r}{\sqrt{(c_2-r)(c_1+r)}} + \frac{\phi_2}{2t}) < 0 \tag{A.7}$$

since $c_1 > c_2$ in our general case for $r \in [0, c_2)$. Thus, $r^{*2\to1} = 0$ always since no transfer is beneficial for SC player 2.

The same analysis can be followed for the general case of $c_2 > c_1 \Leftrightarrow \frac{c_2-c_1}{2\sqrt{c_1 c_2}} > \frac{\phi_2}{\phi_1}$ (players' position interchanged) where it is mutually beneficial only for player 2 to make a transfer. □

A.3 Proof of Theorem 6

For the specific parameters of this case we calculate the expected payoff of T as a function of his own budget allocation across the physical (τ_1) and social (τ_2) battles following Eq. 6.11. Without loss of generality we will assume that the budget relation of the opponents allocated for the physical fight is $\tau_1 < d_1 \Leftrightarrow 1 < \frac{d_1}{\tau_1}$, and for the cyber-social fight $d_2 < \tau_2 \Leftrightarrow \frac{d_2}{\tau_2} < 1$. Therefore the payoff will be:

$$\Psi^T(\tau_1) = \frac{\phi_1 \tau_1}{2d_1} + \phi_2 - \phi_2 \cdot \frac{d_2}{2\tau_2} \overset{\tau_2=\tau-\tau_1}{\Longleftrightarrow} \frac{\phi_1 \tau_1}{2d_1} + \phi_2 - \phi_2 \cdot \frac{d_2}{2(\tau-\tau_1)} \tag{A.8}$$

To calculate the optimal budget allocation for the TO:

$$\frac{\partial \Psi^T(\tau_1)}{\partial \tau_1} = \frac{\phi_1}{2d_1} - \frac{\phi_2 d_2}{2(\tau-\tau_1)^2} = 0 \Leftrightarrow \ldots \Leftrightarrow \tau - \tau_1 = \pm\sqrt{\frac{\phi_2 d_1 d_2}{\phi_1}} \tag{A.9}$$

Since by definition $\tau - \tau_1 > 0$, and ϕ_1, ϕ_2, d_1, d_2 are positive values $\tau_1^* = \tau - \sqrt{\frac{\phi_2 d_1 d_2}{\phi_1}}$, which is a maximum for $\Psi^T(\tau_1)$ as $\frac{\partial^2 \Psi^T(\tau_1)}{\partial r^2} = -\frac{\phi_2 d_2 (\tau-\tau_1)}{(\tau-\tau_1)^4} < 0$. Given that, without loss of generality we assume that the ESA (player 1) transfers budget equal to r to the ICT agency (player 2), while their initial budget is c_1, c_2 respectively. Then the ESA payoff (Eq. 6.11) is:

$$\Psi^1(r) = \phi_1 - \phi_1 \frac{\tau_1^*(r)}{2(c_1-r)} = \phi_1 - \phi_1 \frac{\tau - \sqrt{\frac{\phi_2 (c_1-r)(c_2+r)}{\phi_1}}}{2(c_1-r)} \tag{A.10}$$

Finding the first derivative yields:

$$\frac{\partial \Psi^1(r)}{\partial r} = -\frac{\phi_1 \tau}{2(c_1-r)^2} + \frac{\sqrt{\phi_1 \phi_2}}{4} \frac{(c_1+c_2)}{\sqrt{c_2+r} \cdot (c_1-r)^{\frac{3}{2}}} \tag{A.11}$$

The optimal transfer $r^{*1\to 2}$ is:

$$\frac{\partial \Psi^1(r)}{\partial r} = 0 \Leftrightarrow \frac{c_2 + r}{c_1 - r} = \frac{\phi_2 \cdot (c_1 + c_2)^2}{4\phi_1 \cdot \tau^2} \Leftrightarrow r = \frac{\frac{\phi_2 \cdot (c_1+c_2)^2}{4\phi_1 \cdot \tau^2} \cdot c_1 - c_2}{1 + \frac{\phi_2 \cdot (c_1+c_2)^2}{4\phi_1 \cdot \tau^2}},$$

$$r^{*1\to 2} = \frac{\xi \cdot c_1 - c_2}{1+\xi}, \;\; \xi = \frac{\phi_2 \cdot (c_1 + c_2)^2}{4\phi_1 \cdot \tau^2}$$

Since $r \in [0, c_1)$, $\frac{\partial \Psi^1(r)}{\partial r} > 0$ if $r < r^{*1\to 2}$, and $\frac{\partial \Psi^1(r)}{\partial r} < 0$ if $r > r^{*1\to 2}$, $r^{*1\to 2}$ is a maximum for $\Psi^1(r)$. Thus, if $\frac{\partial \Psi^1(r)}{\partial r}\Big|_{t=0} > 0$ a sufficiently small positive transfer to player 2 will also benefit player 1. This holds iff

$$-\frac{\phi_1 \tau}{2(c_1 - r)^2} + \frac{\sqrt{\phi_1 \phi_2}}{2} \frac{(c_1 + c_2)}{2\sqrt{c_2 + r} \cdot (c_1 - r)^{\frac{3}{2}}} > 0 \Leftrightarrow \ldots \Leftrightarrow$$

$$\frac{c_1 + c_2}{2\tau} > \sqrt{\frac{\phi_1 c_2}{\phi_2 c_1}}$$

which is a necessary condition for the existence of a budget transfer from player 1 to player 2 that is mutually beneficial. To ensure that player 2 is also benefited we can check:

$$\Psi^2(r) = \phi_2 \frac{c_2 + r}{2\sqrt{\frac{\phi_2 (c_1 - r)(c_2 + r)}{\phi_1}}},$$

$$\frac{\partial \Psi^2(r)}{\partial r} = \frac{1}{4}\sqrt{\phi_1 \phi_2} \frac{c_1 + c_2}{\sqrt{c_2 + r} \cdot (c_1 - r)^{\frac{3}{2}}} > 0, \;\; \forall r \in [0, c_1)$$

Therefore, the ICT agency always welcomes a positive transfer from the ESA in this case.

Regarding the opposite transfer ($r^{*2\to 1}$) if we assume that a quantity r is transferred from the ICT agency (player 2) to the ESA then the payoff of player 2 is given by:

$$\Psi^2(r) = \frac{\phi_2}{2} \frac{c_2 - r}{\tau_2^*(r)} = \frac{\phi_2}{2} \frac{c_2 - r}{\tau - \tau_1^*(r)} = \ldots = \frac{\phi_2}{2} \frac{c_2 - r}{\sqrt{\frac{\phi_2 (c_1 + r)(c_2 - r)}{\phi_1}}} = \frac{\sqrt{\phi_1 \phi_2} \cdot \sqrt{c_2 - r}}{2 \cdot \sqrt{c_1 + r}} \tag{A.12}$$

The first derivative:

$$\frac{\partial \Psi^2(r)}{\partial r} = \ldots = -\frac{\sqrt{\phi_1 \phi_2}}{2} \cdot \frac{c_1 + c_2}{\sqrt{(c_2 - r)}(c_1 + r)^{\frac{3}{2}}} < 0 \tag{A.13}$$

$\forall\ r \in [0, c_2)$. Thus, $\Psi^2(r)$ is decreasing in this case and $r^{*2\to1} = 0$ always since no transfer is beneficial for the ICT agency.

The same analysis can be followed for the case where the budget relation of the opponents allocated for the physical fight is $\tau_1 > d_1$, and for the cyber-social fight $d_2 > \tau_2$ (players' position interchanged). Then, it is mutually beneficial only for the ICT agency to make a transfer and for the ESA to accept it. □

Appendix B

Blockchain Mechanisms for Efficient and Secure Smart Grids

The work in this chapter was supported by the US National Science Foundation under the EPSCoR cooperative agreement Grant OIA-1757207. Full versions of these extended abstracts have been published in [67] and [262]. Konstantinos Christidis and Yun Wang, from the Department of Electrical & Computer Engineering, North Carolina State University, have contributed to this work.

B.1 Blockchain Preliminaries

Blockchain relies on a purely distributed and peer-to-peer (P2P) networking topology and can be described as a distributed and transparent public ledger (data structure) replicated and shared among the P2P network entities. Participating nodes, utilize a private public key encryption model to issue transactions (any data exchange) between them. Peer nodes verify the transaction signatures and data before appending them in records termed "blocks" that have specific capacity and consist of a header and a body. The block's body stores the data transactions while the blockchain maintains blocks' chronological order by cryptographically chaining them to their predecessors through the header. The blockchain's first block is known as "genesis" block. Each block's header contains its identifier, that is derived through a cryptographic hash of the included transactions, the previous block's

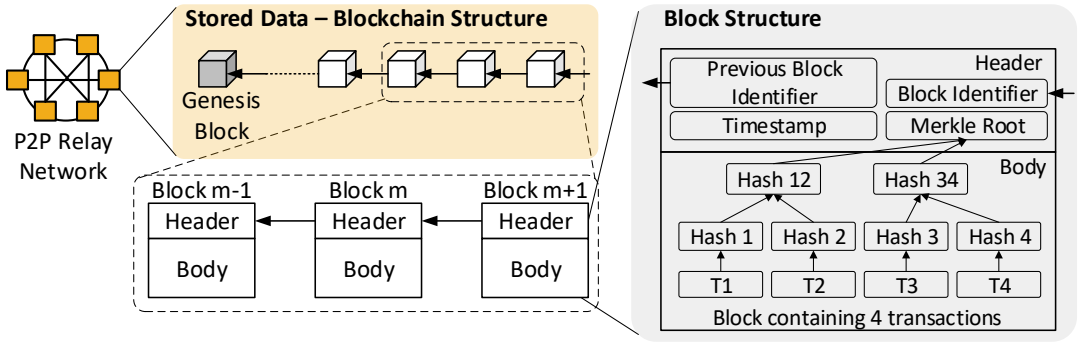


Figure B.1 Blockchain Data Structure

identifier, and a publish timestamp. In addition, the header includes a Merkle tree root that is created by hashing the included transactions' IDs in pairs building a hash tree. Fig. B.1 shows the structure of a blockchain P2P network's components.

Newly created blocks are permanently added to the blockchain using an established set of rules termed distributed consensus protocol that ensures the agreement among the independent nodes of a common global blockchain-data state (transaction content, and order). A variety of distributed consensus algorithms has been proposed (highly active research topic) with diverse impact on the scalability and performance of Blockchain implementations [319]. At a higher level, depending on the specific application and consensus approach, blockchain systems can be either public (permissionless, e.g., Bitcoin) or private (permissioned). In public blockchains any node can take part in the network, issuing transactions, validating and publishing new blocks while maintaining a full copy of the ledger. They usually accommodate large number of nodes and utilize Proof-of-Work (PoW)-based consensus protocols where a miner node collects transactions into a block and only after successfully solves a computationally hard puzzle can append the block into the chain. The aim is to create an environment tolerant to pseudo identities, and malicious behaviour by making any tampering of block contents extremely costly. To the contrary, in private blockchains each node has to be authenticated and strictly identified. Since they admit tighter control on participants and synchronization, they utilize more conventional Byzantine Fault-Tolerant protocols and voting mechanisms to reach consensus without computationally expensive proofs [319].

B.2 Blockchain-based Local Energy Markets

In 2019 through Q3, solar PV accounted for 39% of all new electricity-generating capacity installed in the US [221]. In Q3, 2.6 GW_{dc} of capacity was added – up 45% from the quarter one year-ago –, and the residential sector had its largest quarter ever with 700 MW_{dc} – up 20% year-over-year. In addition, throughout 2018, the median installation price (USD/W) across all market segments fell by 5%, continuing a 5-year trend [27].

The story for battery storage technology is similar: in Q3, 264.6 MWh of battery storage was deployed in the US, marking a 59% quarter-over-quarter increase [311]. Moreover, the residential sector had a record-breaking quarter, with 40 MW_{dc} of newly installed capacity [288]. Across the entire US market, annual storage deployments are expected to reach 5.4 GW_{dc} in 2024, with the market reaching a size of 5.4Bn USD, growing more than 8x from 2019 (645M USD) [311]. Price-wise, costs for lithium-ion battery packs have fallen 85% from 2010 to 2019, to 176 USD/kWh [115], driven mostly by mass production of batteries for electric vehicles.

PV panels and battery storage make a powerful combination; a battery can store excess energy generated by the PV panels during daytime, and make it available to its owner during off-peak hours. As an example, a 5 kWp (kiloWatt peak) PV installation with a 4 kWh battery can double a household's consumption of PV power from 30% to 60% [158].

Effect on utilities

A growing customer base for solar-plus-storage ultimately means less electricity consumed from the grid. Even under the least optimistic modeling scenarios [39], the levelized cost of energy (LCOE) for solar-plus-storage that can meet 100% of a site's load will be cheaper than grid electricity for millions of commercial ratepayers in New York and California by the end of the decade, with grid parity reaching residential customers several years later.

Grid parity aside, demand for power is *already* slowing down. Utilities are already seeing minimal, stagnant, or even negative load growth in their service territories [291]. The reference case (AEO2020) from the most recent Annual Energy Outlook released by the EIA (Energy Information Administration), projects an annual growth in electricity demand that averages just about 1% throughout the projection period (2019-2050) [17].

These trends call for a redesign of the electricity business model. Under the existing regulation, the revenue that utilities make depends directly on the volume of retail sales[1]. Reduced power consumption translates to less profits and the risk of *stranded investment costs* [245]. This leaves the utilities at a dead-end; if they do nothing, their revenues decay; if they penalize the solar customers (e.g., by means of lowering net metering payments or imposing additional fixed charges [146]) —, they may delay revenue loss temporarily, but ultimately will only accelerate the solar-plus-storage trend. Changes in net metering and time-of-use rates *increase* the value of solar energy stored in batteries and discharged later in the day, a dynamic that is already driving battery adoption in Hawaii and Arizona for instance [288].

Transactive energy and performance-based regulation

Proposed business models heavily revolve around two concepts; that of *transactive energy* (TE) [119], and *performance-based regulation* (PBR). In TE, we take advantage of the deployment of two-way communications capabilities and intelligent, communicating sensors and devices and use market-based constructs to dynamically balance supply and demand, while considering grid reliability constraints [283, 306].

With PBR, profits are based on performance goals set by the local Public Utilities Commission (PUC), emphasizing results for customers and system efficiency [309], rather than capital expenditures [172]. Example goals include: reliability (System Average Frequency and Interruption Duration Indexes[2]), peak reduction, power balancing, environmental impact (CO_2/kWh), total cost per customer [134], and customer satisfaction[49].

Smart grid technologies then, turn the utilities into distribution wires companies that become platform service providers. They facilitate the transaction of independent, distributed agents in the electric network, enable experimentation at the grid edge, and lower transaction costs [161].

[1]Remember that the retail rate charged by utilities is a *bundle* of two components: one that covers the utility's investment costs, and one that covers the fuel costs. The latter is revenue neutral, i.e., the utilities do not make money on *the actual energy* they sell [161], but their fixed costs are recovered *through* charges based on how much electricity their customers use [213].

[2]Referred to as SAIFI and SAIDI in the utility industry respectively [3]. SAIFI measures the average number of interruptions per customer per year, while SAIDI measures the average length of each interruption.

This is not merely a theoretical proposition. On the regulatory front, this is the direction that the New York Public Service Commission (PSC) is setting with their "Reforming the Energy Vision" (REV) [49] program. There, utilities operate a retail electricity market where third parties – commonly referred to as third-party grid service providers (GSPs) or energy service companies (ESCOs) – can compete to provide products and services on the retail side, such as energy storage, demand response, and distributed generation [246]. The utilities themselves are rewarded in a PBR fashion[3].

Blockchain-based energy markets

One direction we seem to be headed then, is that of energy markets at the distribution level, that operate on a varying degrees of decentralization. The question that arises is: *how does the underlying transaction management platform*[4] *(TMP) look like?* In our previous work [62], we examined the applicability of blockchains in the Internet of Things (IoT) sector, and as we saw blockchains allow us to build *transparent* digital marketplaces with *verifiable processes*.

Transparency is important because third-party vendors need access to a detailed market load profile and grid utilization data [169]; this allows them to optimize the placement of their distributed energy resources (DERs), and make an informed choice on whether or not they should be participating in a certain market to begin with. SolarCity, a GSP that manages and deploys DERs, has expressed this exact request [2]. Community-choice aggregators in the San Francisco Bay Area shared anonymized customer data with the vendors for that same reason, when soliciting 30 MW of storage-plus-solar capacity last year [287].

Ultimately, transparency lowers the barrier to entry for GSPs and allows them to build more competitive businesses. Verifying the integrity of market processes assuages fears of maladministration by the market operators. As an example, if we are dealing with auctions, we can verify that no late bids were included when they are all published to a blockchain, even if they are encrypted [42]. As another example, consider the case in 2016, where a datacenter operator based in Austin, TX, filed a complaint [192] against the local utility,

[3]Within the REV context this is captured by the Earnings Impact Mechanisms (EIMs) [48] concept.

[4]Recall that this is the layer that handles all market-clearing functions in a way that balances supply and demand in the local market [169].

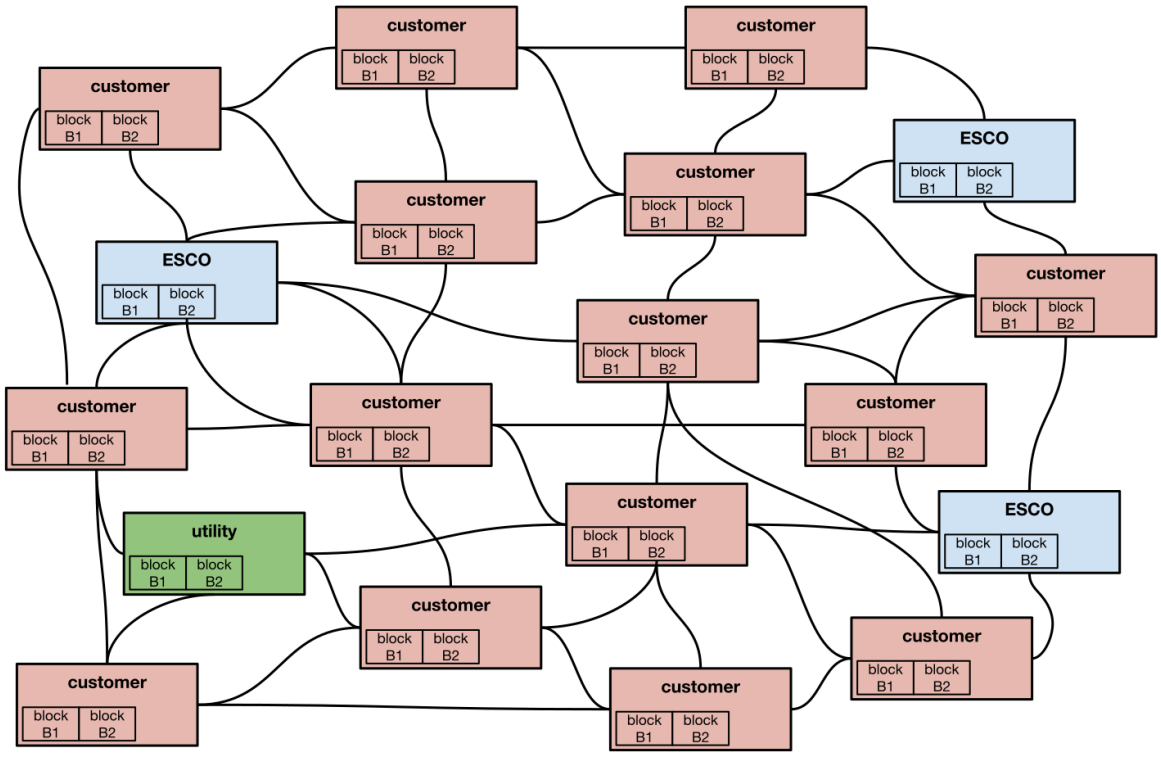


Figure B.2 Conceptual diagram for a blockchain-based local energy market that spans the area served by a distribution substation. Third-party energy service companies (ESCOs) sell services such as distributed generation, storage, or voltage regulation to consumers. Each participant in the system is represented by their own blockchain node. Black lines form the communication network that connects all nodes in the system.

Austin Energy, accusing them of trying to recover the production costs of its wholesale generating business through retail base rates [192][5]. We are not the first ones to suggest that blockchain-based local energy markets (LEMs) (Fig. B.2) *may* work; see [67] for an analysis of all relevant work in the space.

[5]According to the arguments presented in the complaint, Austin Energy attempted to recover the variable production costs associated with its wholesale endeavors twice: once from base rates, and then again from wholesale revenue. The utility would refuse to provide exact revenue figures for its generating business, or a sufficient justification for including its costs in the rate base; as the complaint noted — "AE has the burden of proof, and it failed to carry that burden."

Motivation and Contribution

The problem however with all pieces of existing work in the blockchain-based LEM space is that they focus mostly on the local energy market part, treating the blockchain component as, more or less, a *black box* (see [67]). When setting up a blockchain-based system, a number of questions have to be considered and answered. To name a few:

1. Who runs blockchain nodes, and how are they deployed?
2. Who has read/write-access to the blockchain?
3. What consensus mechanism makes sense? Do all nodes run it?
4. What is the frequency with which blocks are cut? Is the block-cutting frequency configurable? If so, what is its value?
5. Who deploys the smart contracts that expose market primitives, such as "buy" and "sell" orders, and who is allowed to invoke a given smart contract?
6. How is the smart contract designed?
7. What, if any, are the conditions under which the proposed design is subject to tampering by byzantine actors in the market?
8. In case of auctions, what dictates the cut-off time for bids?
9. In case of closed-order book auctions, how are the encrypted bids processed for the market-clearing price to be calculated? How is this price communicated to the market participants?

Depending on the blockchain stack that is used, not all of these questions may apply directly, but the general observation stands: none of the answers to these questions are given, and it is the answers to these questions that dictate whether the proposal makes sense as a blockchain-based application, how that application performs in terms of throughput, and how this affects the market that is provisioned on top of it. Put differently, blockchains reify protocols, and the configuration options offered draw a pretty wide design space.

Questions along the lines stated above *must* be answered, and the answers should also be considered for second-order effects.

In our work in [67], we design a blockchain-based local energy market by carefully considering the questions above, and reasoning over their implications. Specifically:

- We build this market on top of the open-source blockchain platform that we developed and presented in [15].
- We discuss the design of the smart contact that backs the market operations; we identify who deploys the contract, who can invoke it, what its endorsement policy is, what is the considered data model and how it affects performance.
- Given the above, we consider a double auction with closed-order book, and analyze the options available for implementing this mechanism on a blockchain — something that is noticeably absent in the relevant literature.
- We explicitly demonstrate how these design choices matter, by creating three distinct configurations for our local-energy market. Each configuration occupies a different point in the design space: we explain the implications in terms of performance, governance, and degree of decentralization.
- We validate this by performing a case study on the considered configurations, and perform a *joint analysis* on the performance of both the blockchain and the market layers.

Our hope is that the work presented in [67] serves as a guiding framework for designing and evaluating realistic blockchain-based local energy markets. Thus, we have explicitly chosen to focus on how specific blockchain implementation options impact the performance, governance, and degree of decentralization of a next-generation LEM.

Note that this work sets precedence on the blockchain design space definition, and explicitly analyzes its impact on the performance, governance, and decentralization of the LEM. We utilize the open-source blockchain platform Hyperledger Fabric [15] for the blockchain layer of our market, and design and present in detail the underlying *smart contract* architecture, the operational parties, and their roles. We also design and implement

the market mechanism that sits atop the blockchain layer; to the best of our knowledge, our work is the first to explicitly identify *how* a closed-order book double auction can be implemented on a blockchain-based LEM.

Finally, the numerical evaluation demonstrates the applicability of our model to a real-world case, and its ability to provide insights on parameter choices during both market infrastructure planning and day-to-day LEM operation. Our case study, based on residential electricity usage data, showed (subsubsec:case-results-market) how a change in the blockchain data model can decrease the market efficiency by approximately 90%, or — as another example — how a change in the way bids are encrypted can result in further market improvements, but at the risk of subverting the proper operation and resilience of the market.

We consider that the presented work can be adopted as a canonical framework for designing and evaluating blockchain-based LEMs. To that effect, all of the code we have developed and used for this work, including the simulation framework and the local energy market configurations, has been open-sourced [63–65, 68, 69]. Part of our future work includes extending our model to evaluate the use of intelligent market agents, and analyze the market gains that can be had out of this change.

B.3 Blockchain-based Secure Data Exchange

Power system protection is a key grid component responsible for detecting and clearing faults on different equipment, e.g., generators, lines, and transformers [4]. Its key elements are protection relays which are responsible for fault detection and isolation on their protected equipment. A protection system (Fig. B.3) is expected to ascertain requirements for sensitivity (i.e., the ability of timely detecting and isolating faulted regions to avoid damaging other equipment), and selectivity (i.e., the intelligent isolation of faults to minimize the number of customers experiencing power outage). The 2003 Northeast blackout, the world's second most widespread blackout, highlights how a well-coordinated protection system could have prevented the spread of cascading power outages [212]. Also, the 2018 assessment of North American Electric Reliability Corporation reports that 9% of the total grid interruptions in the last five years are related to relay misoperations [211].

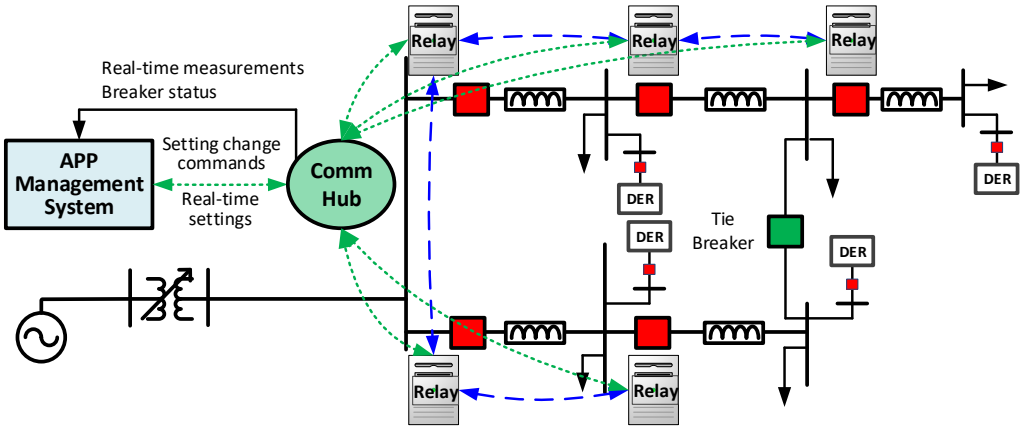


Figure B.3 Adaptive protection platform (APP)

The design of protection systems includes physical components coupled with communication - enabled intelligence to implement the protection logic resulting in large scale cyber-physical formations. Due to the infrastructure's critical role, security is paramount especially since the rapid automation of the grid leads to completely digital protection components with increased capabilities in terms of computing power, embedded storage, and communications. This shift to smart industrial devices, introduces vulnerabilities pertaining to the cyber fabric of the installations that can in turn affect physical components, which is an important national security threat in case critical loads are targeted [279, 295].

Focusing on the cyber layer, power systems automation infrastructure often utilizes centralized communication network with a central substation controller for monitoring data and sending control/protection signals [313]. Such centralized data aggregation creates security challenges as parts of the infrastructure are in risk of being paralyzed in case of an attack on the control center (e.g. 2016 attack against Ukraine's substation [295]). In addition, the emerging digital nature of protection components makes them vulnerable to a series of modern security threats including false data injection attacks [183], grid command tampering (e.g., in Puerto Rico [295]), Aurora attacks, and privacy leaks [295].

Recently, towards enhancing the security of power systems infrastructure, the emerging Blockchain technology [66] has been utilized to achieve build-in privacy, integrity, authenticity, and confidentiality of the exchanged data and control signals. In [124], the authors propose a blockchain-based scheme for smart meter data aggregation within the smart

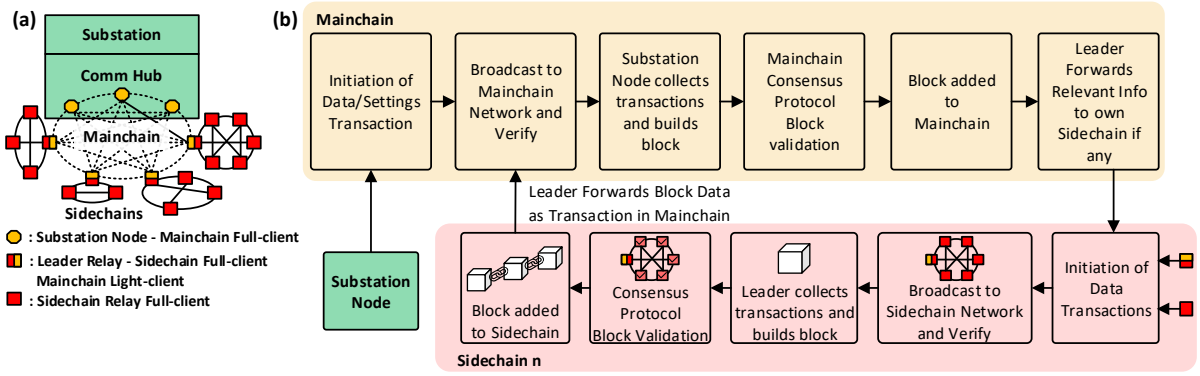


Figure B.4 Multi-tiered Blockchain-based APP Network: (a) Architecture, (b) Workflow Overview

grid to preserve the electricity consumption data privacy by grouping users of the same blockchain network and utilizing pseudonyms for identity protection. However, the final data aggregation is facilitated by traditional means through a wide area network.

In light of the above, our work in [262] introduces a blockchain-inspired network architecture for smart grid relay data aggregation and relay setting dissemination. The main contributions are summarized as follows:

- A scalable Adaptive Protection Platform (APP) is proposed for distribution systems to effectively adjust the protection relays' settings in real-time considering the uncertainties in the power distribution system.
- A multi-tiered decentralized blockchain architecture (Fig. B.4) is adopted to facilitate secure information exchange within the APP. The modular architecture increases the throughput of the local relay to relay communication, while leading to better scalability, and low node storage requirements.
- An analysis of the overall security of the distribution protection system demonstrates how the blockchain-inspired architecture meets various security requirements for measurement aggregation and control signaling.
- An experimental performance evaluation demonstrates that the proposed holistic blockchain-based communication architecture can conclude to a promising solution for future smart grid protection systems.

Appendix C

Quantum-Secure Networking

Extended versions of this chapter were originally published in [267] and in [268].
D. Sikeridis performed this work while at Cisco Systems in collaboration with Panos Kampanakis.

C.1 Introduction

The Internet of the future faces a security threat that stems from the advancements of quantum computing (QC). Indeed, algorithms like Shor's [258] will enable quantum adversaries to solve integer factorization and elliptic-curve (EC) discrete logarithm problems in polynomial time and thus, to break common public key primitives like RSA, (EC)DH, and ECDSA [18, 19, 199]. In response, a standardization process is underway by NIST to identify the next generation of quantum-secure algorithms for key exchange and authentication [216]. Also, organizations like ETSI have formed working groups to develop and study the transition to post-quantum (PQ) cryptography, while the IETF is already working on Internet drafts that propose PQ algorithm integration into existing protocols [102, 293].

Among the first protocols to pay attention to are the critical Transfer Layer Security (TLS), and Secure Shell (SSH). TLS is the most popular secure channel protocol used for mobile apps [238], encrypted access to email servers [139], and web page transfer [56, 164, 209] (∼95% of Google services connections use TLS in HTTPS [117]). The SSH protocol is the primary tool for secure management of remote environments, file transfer, and

private network access [8, 108]. The latest versions (i.e., TLS 1.3, SSHv2) both use (Elliptic Curve) Diffie-Hellman ((EC)DH) for key exchange and RSA or EC signatures. Planning the transition to quantum-resistant schemes is paramount since cryptographic algorithm adoption can take years (e.g., SHA-2 [73, 289], and ECDSA that was barely adopted a decade after standardized [19, 298]).

In light of the above, many industry research teams have been experimenting on the integration of PQ algorithms almost exclusively on TLS. Cases in point include Google, Cloudflare, Cisco, Microsoft, and Amazon with the majority being concerned with PQ key exchange in TLS [37, 45, 170, 171, 175], and secondarily with the PQ signature algorithm integration [219, 268]. Many research teams from Google, Cloudflare, Cisco, Microsoft, and Amazon have been experimenting on PQ algorithm integration exclusively in TLS. They are primarily concerned with PQ key exchange [37, 45, 170, 171, 175], and secondarily with the PQ signature algorithm integration [219, 268]. Apart from the basic prototyping, the focus has been on investigating backwards compatibility with the existing infrastructure (e.g., current middleboxes) and more importantly studying tunnel establishment speeds since the new PQ schemes come with significant overhead due to key/ciphertext/signature sizes and crypto operation speeds. This is important as time-to-first-byte is a critical Quality of Experience (QoE) metric that browsers and cloud service providers strive to minimize.

In this chapter, we complement works that separately study the integration of PQ key encapsulation mechanisms (KEM) [170], or PQ authentication [268], and present a general view on the protocol performance when both are used concurrently. Our contributions are summarized as follows:

- We analyze the TLS 1.3 and SSH handshakes' overhead incurred by using PQ key exchange and authentication.
- We are the first to examine the performance of SSH handshakes when PQ algorithms are used for key exchange and authentication in real-world conditions.
- We experimentally evaluate the performance of the PQ-only TLS handshake in realistic network conditions.
- We determine whether the use of hybrid key exchange (conventional in conjunction with PQ) instead of PQ-only has a material difference on the handshake.

- Finally, we evaluate how adjusting TCP's initial congestion window can reduce the handshake duration of PQ TLS and SSH, and discuss other related optimizations.

C.2 PQ Overhead Analysis

Background

The quantum-secure cryptographic algorithms under standardization by NIST rely on problems that cannot be solved by a quantum adversary faster than a classical one [40], and include secure cryptographic hash functions [24], lattice-based problems [36, 141, 210], and solving multivariate quadratic equations [77], among others. The resulting algorithms demonstrate significant differences among them and compared to traditional pre-quantum cryptographic schemes. Currently, the RSA-2048 and ECDSA are the most commonly used authentication algorithms with keys and signatures between 32 and 256 bytes. This is not the case for the new PQ schemes that lead to slower sign and verify operations, and larger public keys or signatures. Regarding key exchange, ECDH is the current industry standard, with the most popular curve being NIST P-256 with keys of 32 bytes, while the PQ KEMs output keys that vary between 300 and 2500 bytes [312]. Note that key and signature sizes along with the computational cost of all the PQ schemes depend on the specific parameter set and bits of security. NIST has defined five security levels in the range of 128 to 256 bits. The full list of the candidate PQ schemes is available by NIST [216].

In addition, the new PQ signature schemes will affect X.509 certificates that bound digital entities to their public keys verifying each peer's identity [35],[332]. In the current PKI, a set of trusted certificate authorities (CAs) self-sign their own root CA certificates and issue other certificates for intermediate CAs (ICA). Then an ICA is tasked to further sign other ICA or leaf certificates creating a chain of trusted certificates. To validate a leaf certificate at the end of such chain, a digital entity should trust the chain's root CA (public key) and verify the signatures in the chain by using the public key in the issuer's certificate. Currently, the majority of certificate chains on the Internet have lengths of two to three certificates (77% of cases [257]), while the size of a certificate varies between 0.5 and 2 KB. In a PQ era, this size will increase to 4-60KB as the PQ X.509 certificate will carry a PQ public key and the issuer's PQ signature [268].

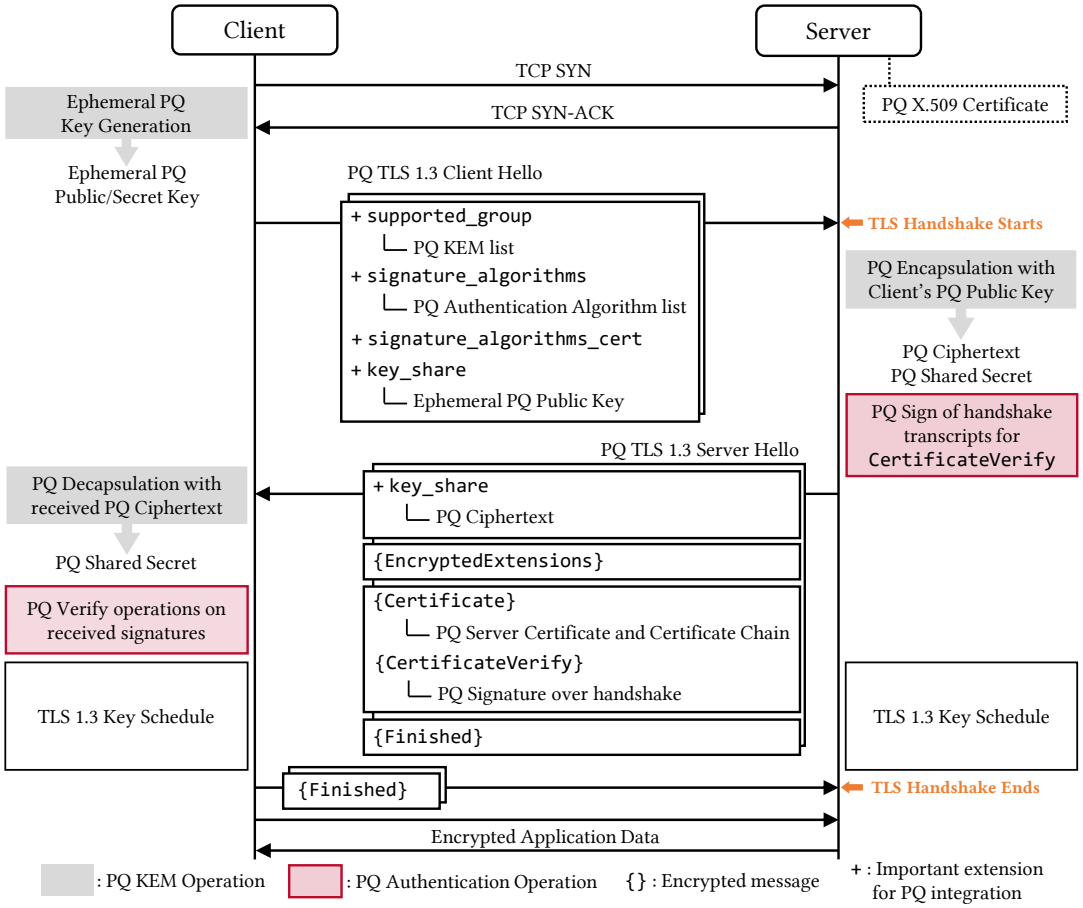


Figure C.1 Post-Quantum TLS 1.3 Handshake Overview

Post-Quantum TLS 1.3 and SSH

The integration of PQ schemes into Internet security protocols affects multiple stages of the handshake procedure. Figures C.1 and C.2 show in detail the fundamental changes within the handshakes of TLS 1.3, and SSH, respectively.

In TLS 1.3 [71, 239], the negotiation of the desired PQ key exchange and signature schemes is facilitated by new identifiers exchanged using extensions in the `ClientHello` message. Since the new PQ schemes are essentially key encapsulation mechanisms (KEM) this procedure is adjusted; the client uses an ephemeral PQ public key as keyshare, while the server — after performing a PQ encapsulation operation against the received public key — responds with the generated ciphertext as its keyshare in the `ServerHello`. In addition,

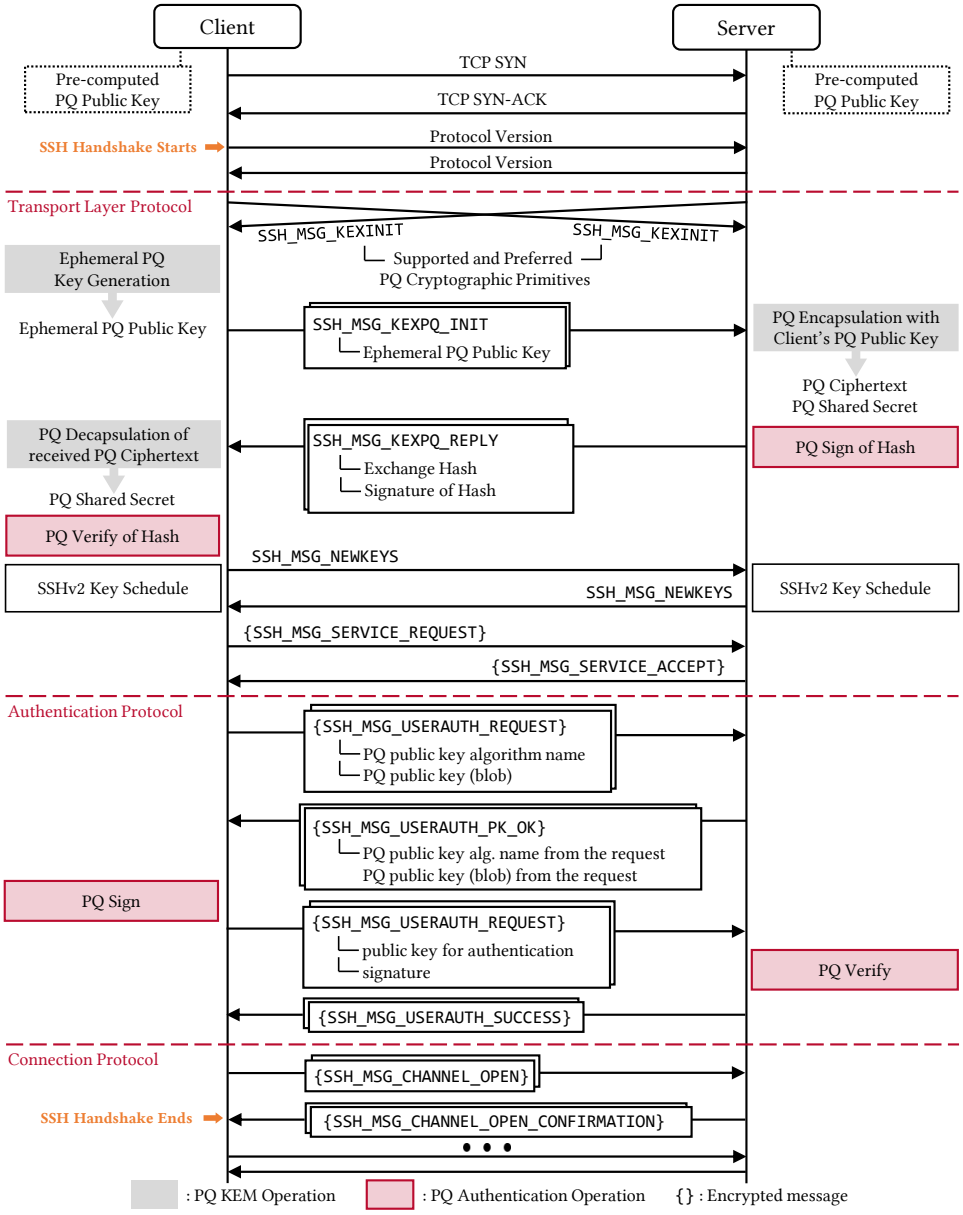


Figure C.2 Post-Quantum SSH Handshake Overview

the server transmits the PQ X.509 certificate chain, and PQ signs handshake transcripts for the `CertificateVerify` message. To end the handshake, the client performs a PQ decapsulation operation of the received ciphertext to produce the PQ shared secret (from the classical and the PQ shared secret) and uses the PQ signature and the certificate chain

to verify the peer's identity. Note that the TLS exchanges tested for this performance study did not perform client authentication and we do not cover it here.

SSH has a different handshake structure that consists of three distinct protocols [186–188]. Initially, both parties sent a `SSH_MSG_KEXINIT` message with the PQ primitives they support. The key exchange procedure is modified to fit the PQ key encapsulation similarly to TLS. A PQ ephemeral key is negotiated using custom `SSH_MSG_KEXPQ_INIT` and `SSH_MSG_KEXPQ_REPLY` messages which include a public key and a ciphertext. In addition, the server proves its identity by performing a PQ signature on the handshake's exchange hash that is followed by the PQ verification at the client's side using the PQ signature algorithm negotiated previously. The rest of the SSH handshake remains the same leading up to the exchange of the new keys (`SSH_MSG_NEWKEYS` message). Next, the default SSH authentication protocol takes place (client key-based authentication) with the client transmitting an authentication request containing the desired PQ signature algorithm accompanied with its PQ public key. After the server's agreement, the client performs and sends a PQ signature over the handshake transcript [186]. Finally, the server performs a PQ verify operation on the received signature, and sends a `SSH_MSG_USERAUTH_SUCCESS` before initiating the SSH connection protocol [187].

C.3 Performance Evaluation and Discussion

Experimental Setup

In this subsection, we describe our experimental setup along with the specific algorithm choices. The PQ algorithm integration into SSH and TLS was performed using the OQS OpenSSH [229], and OQS OpenSSL libraries [230] that were based on OpenSSH 7.9, and OpenSSL 1.1.1c versions, respectively. They utilize the liboqs [228] library which implements the new PQ schemes with AVX2 optimized versions.

The experimental testbed consisted of a local host and three remote servers running Ubuntu 18.04 in x86_64 architecture. The local client was equipped with an Intel i7-8665u that utilized four cores at 1.9 GHz each, and 8 GB of RAM, while the remote servers were e2-standard-2 Google Cloud [271] instances equipped with an Intel Skylake Xeon (2 cores at 2.0 GHz) and 8 GB RAM. Each VM-server was located at increasing proximity from the

Table C.1 Details of Key Exchange Algorithms and Parameter Sets used in our experiments

Key Exchange Algorithm	Notation	Problem Family	NIST PQ Security	Public Key (Bytes)	Secret Key (Bytes)	Ciphertext (Bytes)	Key gen. (ms)	Encaps. (ms)	Decaps. (ms)	Optimization
ECDH NIST P-256 [18]	`ecdhp256`	EC Discrete Logarithm	≈0 bits	32	32	32	0.13 (7510.70 op/sec)			OpenSSL
ECDH NIST P-384 [18]	`ecdhp384`	EC Discrete Logarithm	≈0 bits	48	48	48	1.95 (512.30 op/sec)			OpenSSL
Kyber-512 [36]	`kyb512`	Module LWE	Level 1	800	1632	736	0.09	0.08	0.06	AVX2
NewHope-512-CCA [11]	`nh512`	Ring LWE	Level 1	928	1888	1120	0.09	0.09	0.07	-
Kyber-768 [36]	`kyb768`	Module LWE	Level 3	1184	2400	1088	0.13	0.12	0.10	AVX2
NTRU-HRSS-701 [141]	`hrss`	NTRU	Level 3	1138	1450	1138	10.18	0.43	1.18	-

Table C.2 Details of Signature Algorithms and Parameter Sets used in our experiments

Signature Algorithm	Notation	Problem Family	NIST PQ Security	Public Key (Bytes)	Private Key (Bytes)	Signature (Bytes)	Sign (ms)	Verify (ms)	Optimization
RSA 2048 [199]	`rsa2048`	Integer Factorization	≈0 bits	259	256	256	0.54	0.02	OpenSSL
Dilithium *III* [81]	`dil3`	Module LWE	Level 2	1472	3504	2701	0.32	0.22	AVX2
SPHINCS$^+$ SHA256-128f-simple [24]	`sph128`	Hash-Based	Level 1	32	64	16976	15.93	1.98	AVX2
Dilithium *IV* [81]	`dil4`	Module LWE	Level 3	1760	3856	3366	0.38	0.28	AVX2
SPHINCS$^+$ SHA256-192f-simple [24]	`sph192`	Hash-Based	Level 3	48	96	35664	26.99	4.14	AVX2

local client as follows:

- *Close* range: Average RTT of 37 ms, 13 hops
- *Intermediate* range: Average RTT of 67 ms, 16 hops
- *Long* range: Average RTT of 163 ms, 24 hops

Note that the intermediate distance represents the majority of connections as seen in Firefox TLS handshake data (median of 62.25 ms from ≈56 million samples of the nightly 78 version [202]). In addition, previous related studies utilize a similar RTT range in their experiments [219, 268]. Finally, the experiment scenarios were as follows: For TLS the host performs 1-RTT mode handshakes with the server without PSK resumption. Only the server is authenticated with X.509 certificates that do not include SCT, OCSP, or CRL extensions. The server certificate chain has one ICA (majority case [257]). For SSH, the client and server are using key-based authentication. The default TCP initial window (`initcwnd`) of 10 MSS was initially used in all cases.

Regarding our use of PQ schemes, the 9 PQ signature and 17 PQ KEM algorithms under NIST consideration in Round 2 give a minimum of 153 possible combinations without

accounting for all the different parameter sets and security levels [216]. Since (a) benchmarking all combinations is out of the scope of this work, and (b) the characteristics of some algorithms deem them less favorable for TLS and SSH as shown in [268] we use a subset of chosen representatives. For authentication, we chose two algorithms that have both AVX2 optimized implementations [1]. *Dilithium* [81] represents the family of lattice-based signature schemes that are the most promising in terms of performance but rely on relatively new and immature hard problems [2]. We also test *SPHINCS*$^+$ [24] which is a hash-based scheme, with larger signatures and computationally heavier. However, hash-based signatures are well-understood and trusted. As for PQ key exchange, the majority of schemes rely on lattices and present similarities in terms of key sizes and computational cost. We use *Kyber*, which is the only AVX2 optimized KEM scheme currently in liboqs, and for comparison we also tested *NewHope* for level 1 security, and *NTRU-HRSS* for level 3 (*NewHope* defines parameter sets only for NIST security levels 1 and 5, while *NTRU-HRSS* only for NIST security level 3). Finally, for our conventional security **control** group we use RSA 2048 for authentication, and ECDH with the NIST P-256 curve for key exchange. Tables C.1, and C.2 summarize the details of the signature and KEM algorithms used, respectively.

PQ-only TLS Handshake Overhead

Our client performed 5×10^3 PQ-only TLS handshakes with each remote server distributed uniformly within 24 hours. The attempted handshakes had a success rate of 100% without any middlebox malfunction due to the increased certificate size. Figures C.3 and C.4 show the 50th and 95th percentiles of the TLS handshake completion time for the examined security levels. As the results indicate the two PQ KEMs of choice have a minimal impact on the handshake duration with latencies that range between 0.1 and 5 ms for `nh512` and `kyb512` and between 1 and 4 ms for `hrss` and `kyb768` at the median across all client-server distances. This is not the case for all PQ signature algorithms tested, although the lower security combinations that use `dil3` are competitive against the control pair by introducing a 0.6% to 2% increase in latency at the median regardless of the distance. This result, is

[1] See the work in [268] for more information on the impracticality of certain PQ signature algorithms.

[2] We used the *Dilithium 3* variant —of Level 2 security— since the conventional security (CoreSVP problem) of the Level 1 parameter set is ~100 bits, and it is therefore lower than the most commonly used 128 bits of security parameter sets today

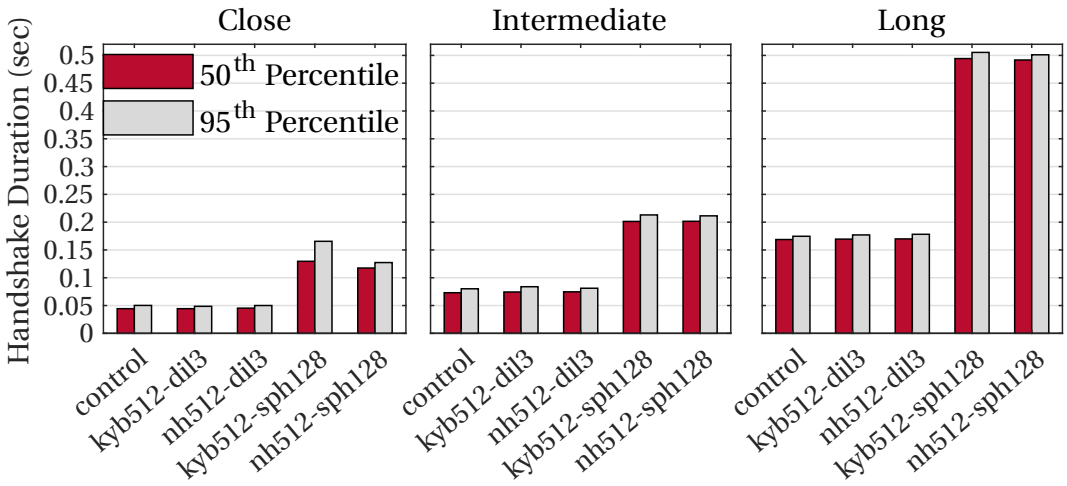


Figure C.3 PQ-only TLS 1.3 Handshake - NIST Level 1,2

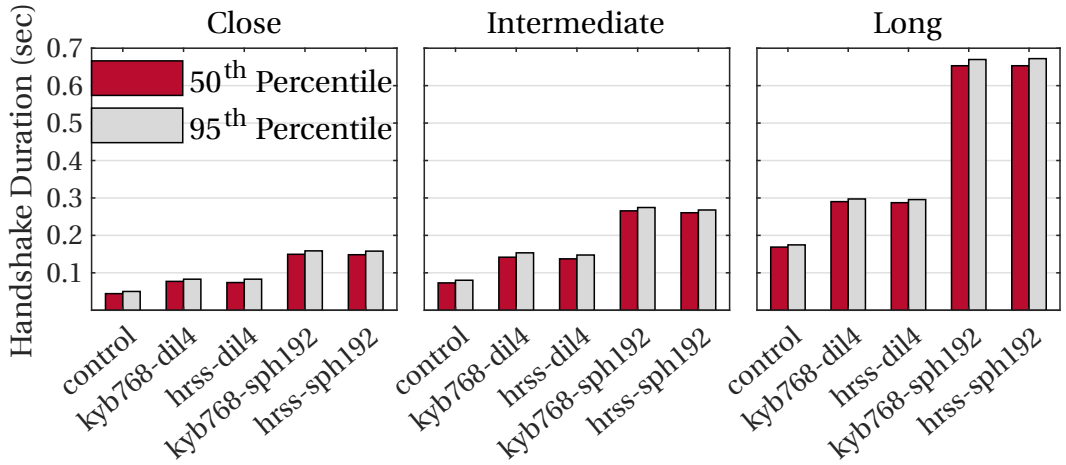


Figure C.4 PQ-only TLS 1.3 Handshake - NIST Level 3

slightly more optimistic, but generally aligned with the findings in [171, 268]. The use of `sph128`, however, increases this gap to a 150% latency increase for the close server and 190% for the distant one. This is attributed to the computationally heavier signing and the larger `sph128` certificates whose transfer requires more round-trips due to the TCP `initcwnd`. Similar performance degradation is observed for the level 3 security signature schemes, where the client will have to tolerate a latency increase of 75% (`dil4`) to 300% (`sph192`) at the median when compared to the control pair.

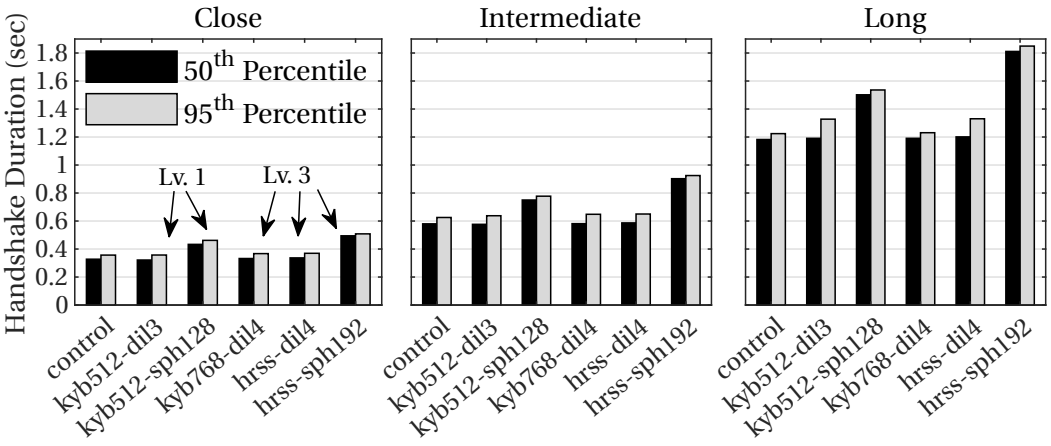


Figure C.5 PQ-only SSH Handshake - All NIST Levels

PQ-only SSH Handshake Overhead

Again, we performed 5×10^3 PQ-only SSH handshakes per server uniformly distributed within a day, and received a 100% success rate in SSH session establishment. Figure C.5 shows the 50% and 95% percentiles of the observed SSH handshake time. The results indicate that across all server distances the majority of PQ algorithm pairs increase the handshake duration by ≈1-8ms while in some cases slightly outperform the control pair —e.g., `kyb512-dil3` in close range led to 2% handshake time reduction—. The latter is probably because `kyb512` is marginally faster than `ecdhp256` and `dil3` signing is slightly faster than `rsa2048` signing. At the same time, in this case, no extra round-trips are introduced during the PQ SSH handshake, and therefore crypto operations are the main differentiation factor over the control pair. For longer network routes, however, the conventional schemes still outperform the PQ ones at the 95th percentile due to increased packet loss and retransmissions. The same holds for the cases that involve SPHINCS$^+$ parameter sets which produce a slowdown that ranges between ≈30% (`kyb512-sph128` for close proximity) to ≈50% (`hrss-sph192` for long distance) over the control pair. This slowdown is caused by the slower SPHINCS$^+$ signing (28-49 times slower than RSA) that happens twice in the SSH handshake, and by the two exchanged signatures that add extra round-trips per handshake. We should note that while there were no handshake failures, we observed unexpected packet delays (potentially from middleboxes) for longer bursts of traffic (average delay of

Table C.3 TLS Handshake: Hybrid Key Exchange Impact

Algorithm Combination	TLS Handshake (ms)			Latency over control (%)		
	Mean	50^{th}	95^{th}	Mean	50^{th}	95^{th}
ecdhp256-rsa2048 (control)	72.59	72.58	76.48	-	-	-
ecdhp256+kyb512-rsa2048	73.17	73.05	77.27	0.79	0.65	1.03
ecdhp256+kyb512-dil3	74.27	74.12	78.23	2.31	2.12	2.28
kyb512-dil3	73.59	73.43	78.12	1.38	1.17	2.14

Table C.4 SSH Handshake: Hybrid Key Exchange Impact

Algorithm Combination	SSH Handshake (ms)			Latency over control (%)		
	Mean	50^{th}	95^{th}	Mean	50^{th}	95^{th}
ecdhp384-rsa2048 (control)	583.87	575.21	600.47	-	-	-
ecdhp384+kyb512-rsa2048	588.99	579.95	625.39	0.88	0.82	4.15
ecdhp384+kyb512-sph128	771.57	763.49	790.95	32.14	32.73	31.72
kyb512-sph128	755.89	750.24	777.55	29.46	30.43	29.49

60ms for the SPHINCS$^+$ cases). We also saw that an ACK was sometimes reaching the client or server quickly while it was sending data to fill up the TCP congestion window which led it to increase the window and thus prevented a round-trip.

Impact of Hybrid Key Exchange

The majority of experimental work on the PQ key exchange follows the hybrid approach where the PQ KEM is combined with a conventional key exchange algorithm [294]. Such implementations negotiate the KEM pair as a separate key exchange algorithm and concatenate the two (e.g., PQ and ECDH) shared secrets [73]. The two shared keys are used as one in the place of the ECDH secret in the TLS or SSH key schedule. This practice provides confidence that the key is secure as long as either algorithm is secure and enables the early adoption of the PQ KEM schemes since PQ confidentiality is more urgent than authentication; impersonation cannot happen retroactively before the existence of a quantum machine, while the decryption of recorded communications can take place after a

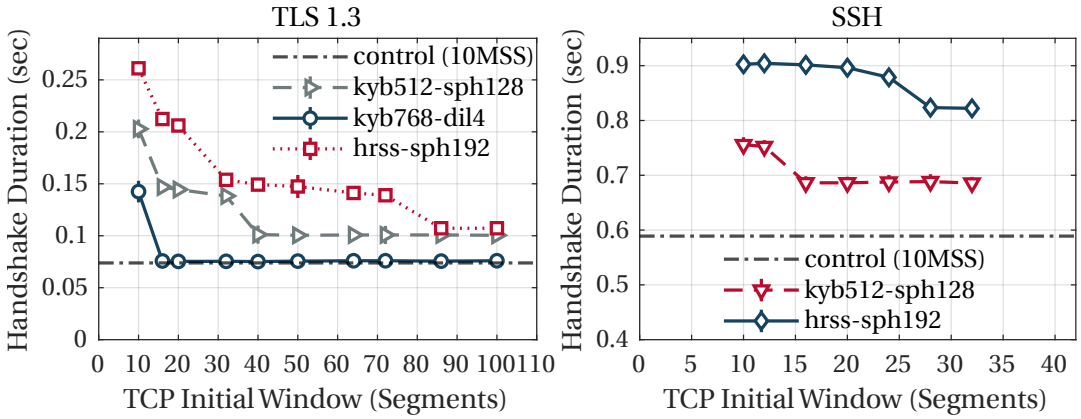


Figure C.6 Average Handshake Completion Time vs TCP Initial Window Setting (`initcwnd`) - (Left) TLS 1.3, (Right) SSH

QC is a reality. Therefore, we examine whether this transitional practice is a significant burden to the TLS and SSH handshake. Table C.3 shows the performance of all the possible combinations of using a hybrid KEM with ECDH P256 and the AVX2-optimized `kyb512` in TLS 1.3. The same setup and client were used with the intermediate distance server (RTT ≈ 67ms). Results show that the addition of hybrid key exchange instead of PQ-only delays the handshake by ≈1ms which is negligible. The same behavior is observed in the SSH handshake —Table C.4— where the average additional latency of the hybrid key exchange is less than 2% over the PQ-only case.

Adjusting TCP's initial window

Our findings indicate that the performance of some PQ schemes heavily depends on the behavior of TCP and specifically on its initial congestion window (`initcwnd`) size. This parameter defines the number of bytes sent unacknowledged after the TCP handshake and influences the rest of the connection as it enters the TCP slow start [248]. The `initcwnd` is expressed either in bytes or multiples of Maximum Segment Size (MSS) where 1MSS=1460 bytes assuming 1500-byte maximum transmission unit (MTU). Thus, to examine its impact on the PQ-only versions of TLS and SSH we repeated the experiments while adjusting the Linux standard 10MSS `initcwnd`. Figure C.6 shows the average handshake completion time for TLS and SSH as the `initcwnd` value increases both for client and server (intermediate distance). When the window is small the long certificates (TLS) and signatures (SSH) of

schemes like dil4, sph128, sph192 exceed it. This prolongs their transmission as TCP is forced to wait for ACKs before increasing the window, and thus extra round-trips are added to the handshakes. Results show that by increasing initcwnd by even 4MSS we eliminate some latency and achieve a decrease in the TLS handshake duration (19-50% depending on the scheme) while for larger windows (e.g., 86MSS) this drop reaches 60% for the SPHINCS$^+$ pairs reducing the gap from the control pair. The same behavior holds for SSH where by increasing initcwnd the handshake times are reduced by 70-80 ms. We should note that an imprudent increase of the initcwnd can increase the loss rate in cases of congested or low bandwidth connections. RFC3742 [101] and RFC6928 [70] raise related concerns for the adverse effects in lossy environments or developing regions. This would also affect all applications running over TCP even 3rd party TCP connections traveling over the same infrastructure without using TLS or PQ authentication. The last —highly-debated— change in the recommended window size by IETF took place in 2013 [70] due to the increasing page sizes and Internet speeds [82]. Recent studies [249] show that initcwnd customization is not uncommon (up to 100MSS) for some Content Distribution Networks, while the majority uses the standard 10MSS value. A future increase in the recommended window value could aid the adoption of more PQ schemes in TLS and SSH. Our measurements show that servers could aim for up to 75MSS and 27MSS initcwnd for sph192 in TLS and SSH respectively.

Lessons Learned and Other Optimizations

Our measurements prove that post-quantum TLS 1.3 and SSH are possible with relatively good performance assuming the use of proper algorithms. Lattice-based KEM schemes which have relatively small public keys and ciphertexts (≈1KB) with fast crypto operations (<1ms) could be used in conjunction with classical algorithms for hybrid key exchanges. Examples include Kyber, NTRU, Round5, and NewHope [216]. Signature schemes with signatures and public keys of a few KBs with fast signing and verification are appropriate for authentication, as long as no round-trips are introduced in the handshake or such overhead is not detrimental. For instance, applications that rely heavily on TLS for establishing short and fast connections will be impacted more from the PQ transition than those where tunnels stay active longer as in many SSH usecases.

For completeness, we note that our SSH results would vary based on the client authen-

tication method. Client password authentication would eliminate one PQ signature and PQ public key transfer, thus it would be faster. Measurements indicate that `sph128` at the server and password at the client suffers only a ≈15% slowdown from classical SSH instead of ≈30% in our results with client key-based authentication. On the other hand, using PKI certificates for authentication in SSH will introduce more round-trips because of the extra keys and signatures in the certificate chain (as in TLS 1.3).

A simple optimization to decrease the PQ data transferred in an SSH handshake with client key authentication is omitting the `SSH_MSG_USERAUTH_REQUEST` message that carries the client public key separately. The key is included in the subsequent `SSH_MSG_USERAUTH_REQUEST` along with the signature anyway. SSH's RFC 4252 [186] does not mandate sending the public key for authorization separately before sending the signature. Omitting it at the client, and performing the authorization check at the server before verifying the signature is trivial and can save significant data transfer overhead when the PQ signature scheme uses large public keys.

Regarding TLS, it is evident that PQ signatures will be a handshake performance bottleneck in case lattice-based authentication schemes are not standardized especially for the Web. To alleviate the issue, omitting ICA certs [240, 304] or certificate compression [111] could reduce the handshake's bandwidth usage during the certificate transfer without altering the protocol's state machine [72].

The integration of PQ crypto algorithms in network security protocols will affect multiple aspects of the underlying systems that use them. This work focuses on the additional latency that will be introduced in client-native applications that utilize TLS or SSH connections frequently, and can impact the Quality of Experience of users. On the server-side, the slower PQ operations can also reduce the throughput of a server performing PQ authentication and key exchange. Detailed analysis of the impact of PQ authentication on server throughput (amount of established connections per second) can be found in [268] which showed that heavily loaded server throughput is mainly affected by algorithm processing instead of PQ handshake data. Furthermore, additional memory requirements due to the PQ algorithms can be another point of interest for both clients and servers. The work in [156] discusses stack memory implications in ARM Cortex-M4 microcontrollers and shows that the schemes we experimented in this work fit in high-end microcontrollers without an issue. Finally, the integration of the new PQ schemes in libraries for embedded systems [43] and constrained

devices raises concerns related to battery lifetime and power consumption. In this regard, a detailed analysis of energy requirements of PQ crypto candidate algorithms on a ARM Cortex-M4 can be found in [250]. This work reveals that lattice-based algorithms like the ones we experimented in this paper offer good performance for cloud-connected mobile devices even when per-bit data transmission energy cost is relatively high.

C.4 Related Work

Since the announcement of the NIST PQ algorithm candidates, research teams have been working on prototyping PQ internet security protocols. The PQClean [292], and Open Quantum Safe (OQS) [231] projects provide PQ algorithm implementations and a library with a common interface to simplify integration. OQS also provides OpenSSL and OpenSSH forks customized to include PQ schemes. Crockett, et al. [73], discuss these implementations and the challenges involved.

Regarding PQ protocol performance experiments, most tackle only TLS and focus either on testing the impact of PQ key exchange or PQ authentication separately. In 2016, Google initiated an experiment for hybrid key exchange (conventional ECDH *and* PQ KEMs) in TLS using the NewHope [11] scheme (CECPQ1 [174]). More recently, Google in collaboration with Cloudflare modified Google Chrome browsers to test hybrid key exchange in TLS 1.3 [170, 171, 175]. Their highly realistic network setup tested two NIST PQ KEM candidates, namely the NTRU-HRSS (CECPQ2 [175]), and SIKE (CECPQ2b [170]). Both experiments used standard non-PQ certificates and ECDSA (X25519 curve) for authentication.

In the opposite scenario, a team from Cisco tested the impact of PQ signature schemes on the TLS 1.3 handshake while using conventional ECDH (secp384r1 curve) key exchange [154, 268]. Their experiments examined the impact of six PQ signature schemes on the TLS handshake and server performance. Focusing more on PQ signatures, Kampanakis et al. discussed the impact of PQ signature schemes on protocols that utilize X.509 certificates in [153]. They considered the case of hybrid certificates that include hash-based signatures, and conducted performance experiments on TLS 1.2 and IKEv2. Also, their work discussed the use of PQ certificates by emulating their increased size through enlarging certificate chains with additional certificates. On the same topic, earlier work by Bindel

et al. emulated large hybrid PQ certificates and studied their impact on TLS libraries and browsers [34] Paquin et al. [219], on the other hand, proposed a framework to run PQ cryptography experiments on the TLS handshake while emulating packet loss and link latency. They considered two cryptographic scenarios; conventional ECDSA (NIST P-256 curve) with hybrid key exchange (SIKE, Kyber, and FrodoKEM), and conventional ECDH (NIST P-256 curve) with PQ signature schemes (Dilithium, qTesla, and Picnic).

Finally, the work in [43] measured PQ-only TLS runtimes in constrained embedded devices by integrating the PQ signature algorithm SPHINCS$^+$ and the PQ KEM Kyber in an *embedded* TLS library. However, the focus is clearly on the PQ handshake feasibility on embedded systems without accounting for transfer time, and network conditions.

We did not find any work investigating the performance impact of PQ KEM and signature schemes on the SSH handshake.

C.5 Conclusion

In this chapter, we experimentally assessed the concurrent use of quantum-resistant key exchange and authentication in TLS 1.3 and SSH protocols. We use combinations of representative post-quantum schemes and monitor client-server handshakes under realistic network conditions. Our measurements reveal a subset of PQ scheme pairs that offer competitive handshake performance against the current standards with a minimum slowdown of $\approx 1\%$ for both protocols. The same holds for the use of hybrid key exchange which is considered the first step towards PQ security and introduces $\approx 1\%$ handshake latency. Finally, we underline and evaluate the impact of the TCP initial window size on the PQ scheme integration. We show that even a small increase in window size can reduce the observed slowdown by even 50%. Future work will investigate the PQ authentication and confidentiality impact on protocols like IKEv2/IPsec, and examine performance optimization options. We are hopeful that this paper will provide practical feedback to NIST's standardization process and will serve as a baseline as quantum-secure Internet becomes a reality [155].