Enabling Cyber-Physical Communication in 5G Cellular Networks: Challenges, Solutions and Applications

By

Rachad Atat

Submitted to the Department of Electrical Engineering and Computer Science and the Graduate Faculty of the University of Kansas in partial fulfillment of the requirements for the degree of Doctor of Philosophy

Lingjia Liu, Chairperson

Yang Yi, Co-Chairperson

Committee members

Shannon Blunt

James Rowland

Jin Feng

Date defended: June 14, 2017

The Dissertation Committee for Rachad Atat certifies
that this is the approved version of the following dissertation :

Enabling Cyber-Physical Communication in 5G Cellular Networks:
Challenges, Solutions and Applications

Lingjia Liu, Chairperson

Yang Yi, Co-Chairperson

Date approved:

Abstract

Cyber-physical systems (CPS) are expected to revolutionize the world through a myriad of applications in health-care, disaster event applications, environmental management, vehicular networks, industrial automation, and so on. The continuous explosive increase in wireless data traffic, driven by the global rise of smartphones, tablets, video streaming, and online social networking applications along with the anticipated wide massive sensors deployments, will create a set of challenges to network providers, especially that future fifth generation (5G) cellular networks will help facilitate the enabling of CPS communications over current network infrastructure.

In this dissertation, we first provide an overview of CPS taxonomy along with its challenges from energy efficiency, security, and reliability. Then we present different tractable analytical solutions through different 5G technologies, such as device-to-device (D2D) communications, cell shrinking and offloading, in order to enable CPS traffic over cellular networks. These technologies also provide CPS with several benefits such as ubiquitous coverage, global connectivity, reliability and security. By tuning specific network parameters, the proposed solutions allow the achievement of balance and fairness in spectral efficiency and minimum achievable throughout among cellular users and CPS devices. To conclude, we present a CPS mobile-health application as a case study where security of the medical health cyber-physical space is discussed in details.

Acknowledgements

First and foremost, I would like to thank God for embracing me in His mercifulness and care throughout all my life, especially in my Ph.D. journey and the difficult times I have been through. Without my family's support, sacrifices and ultimate care, I would have not been able to complete my doctoral degree. So, I thank each one of them: my amazing mom, Salwa El-Zein, for her endless support and care about me getting the best education and a bright future since the primary school up to this stage of my life; my caring father, Ramez Atat, who finds it hard to sleep without fully knowing that I am safe and in good shape; my brothers Jawad and Ziad for their moral, financial and endless support in the last years; and for my aunties, uncles and cousins for their encouragement and love.

I would like to thank my advisors Dr Lingjia Liu and Dr Yang Yi for their mentorship and support. I specially thank Dr Liu for caring about me as a person first and as his student second, as well as his care and support for my future. I also thank him for carefully listening to my ideas, thoughts and feelings, and for introducing me to all the highly respectful and skillful researchers from both academia and industry, whom I had the chance to collaborate with. I also extend my thanks to all the professors whom I had taken classes with, especially my committee members who agreed to supervise and judge my work.

Lastly, I thank all my colleagues in the office, without whom, researching and coming up with new ideas would have been difficult tasks. I thank them for also being close friends of mine, for sharing our thoughts, and for hanging out together.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Cyber-physical communications (CPS) has been under the spotlight of attention in the last decade by the research community and the industry. CPS allows physical objects to tightly interact and coordinate together to provide ubiquitous services in a myriad of applications including but not limited to health-care, public safety, environmental management, vehicular networks, industrial automation, and so on. A CPS is defined as a system with integrated communication and computational capabilities with tight interactions with the physical world [4]. It mainly consists of physical components and a cyber twin interconnected together, where a cyber twin is a simulation model representative of the physical things such as a computer program [5]. Internet of Things (IoT), on the other hand, allows different CPS to be connected together for information transfer. This means that IoT acts as a connection bridge to network different cyber-physical things. The global expansion of interconnected CPS is facilitated by standardization efforts. For instance, the standardization activities of IoT are being led by the industry (AllSeen Alliance, Open Interconnect Consortium, Industrial Interconnect Consortium) and IEEE P2413 project on standards specifications of IoT architecural framework [6]. The ”things” such as users, sensors, Radio-Frequency Identification (RFID), devices and applications, are interconnected together either directly or through

a gateway device, providing seamless connectivity to objects located in different locations of the world [7]. Machine Type Communications (MTC), Low power Wireless Personal Area Networks (LoWPAN), wireless sensor networks (WSN) and RFID are some of the concepts related to CPS. These different networks are characterized by large amount of traffic with smart decision making with little or no human interaction. For instance, the number of MTC devices is in continuous growth, with an estimation of 50 billion devices to be connected by the year 2020 [8, 9]. This expected massive growth of machine devices will bring revenues of more than 300 billion dollars in the next 5 years [10], with a share of 3.1 % of the total mobile subscriptions [8].

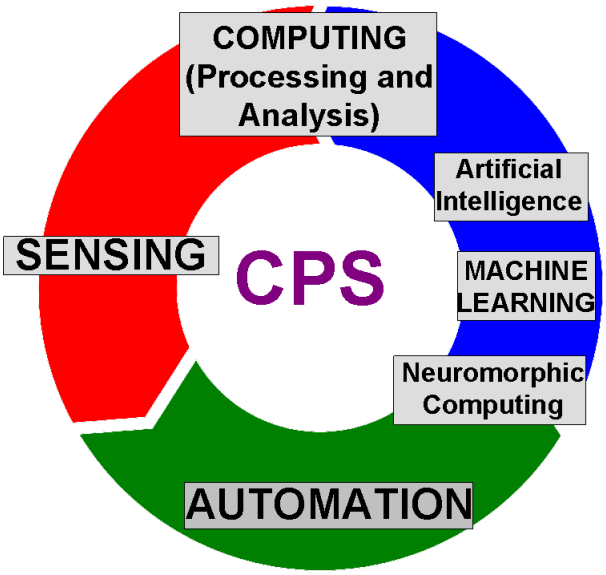

Figure 1.1: CPS cycle to automation.

When CPS is combined with artificial intelligence, machine learning, and neuromorphic computing techniques, it is envisioned that new applications will be developed with automated decision making, which would revolutionize the field of smart cities, industrial plants, environmental monitoring and others (see Fig. 1.1). Examples of such applications include but not limited to healthcare, where patients' information can be accessed using a cloudlets-based infrastructure [11]. Cloudlets are clouds that are closer to users to help overcome the high latency and power consumption of distant clouds [12]. Other cloud application examples include vehicles traffic control system [13], genome analysis [14], earth surface analysis [15] and many others.

With CPS creating a tsunami of new information, also known as big data, the revenues of many businesses can be boosted by identifying customer needs and providing them with superior services. However, this enormous amount of data is so large in size and complex in real-time that it exceeds the processing capacities of conventional systems. That is why, cloud computing techniques along with machine learning tools, data mining, artificial intelligence, and fog computing can help the sensed data be easily stored, processed, and analyzed to uncover hidden patterns, unknown correlations and other useful information [16]. That is why big data is referred to as "*the 21st century new oil*".

On the other hand, interests and technical discussions about emerging technologies for the fifth generation (5G) cellular network have evolved into a full-fledged conversation capturing attention from researchers across the world [17]. It is envisioned that 5G technologies will be able to expand and support diverse usage scenarios and applications. To be specific, the usage low latency communications (URLLC), and massive machine-type communications (mMTC) [18]. For URLLC, the use case has stringent requirements for capabilities such as throughput, latency, and availability. Some examples include wireless control of industrial manufacturing or production processes, remote medical surgery, distribution automation in a smart grid, transportation safety, and so on. For mMTC, the use case is characterized by a very large number of connected devices typically transmitting a relatively low volume of non-delay-sensitive data. Devices are required to be low cost, and have a very long battery life requiring energy-efficient communication and computing. For the communication side, it is shown that local/short-range communication could significantly improve both the energy efficiency and spectral efficiency of a wireless system when circuit energy consumption is considered [19, 20]. For the computing side, the recent developed concept of neuromorphic computing/ reservoir computing can be a great candidate to significantly reduce the energy consumption [21, 22].

It is clear that the URLLC and mMTC aspects of 5G are clearly related to CPS and 5G cellular network may provide an ideal platform for CPS communications. On the other hand, enabling CPS communication in 5G cellular networks is far from being straightforward. For example, supporting

coexistence between cellular users (CUs) and CPS links requires many new functionalities and control overhead which significantly complicates the network design.

First, current cellular networks are not designed to handle large volume of traffic, as CPS devices will rapidly cause congestion in the network from excess signaling overhead, leading to a failure of many of these communications. Second, the number of radio resources is already scarce and limited for traditional human communications; how about the anticipated massive number of devices? This means packet scheduling problems will occur and the network capacity and spectral efficiency will significantly degrade [23]. Third, there is a concern of excessive interference generated from the massive number of devices, add to that the multipath fading, which all lead to a performance degradation due to wireless channels becoming unreliable. So it is evident that we are facing several challenges when it comes to enabling CPS communications over current cellular networks; however many of these challenges can be addressed by the specifications and technologies of future 5G networks, as was discussed in [24].

For instance, to support massive machine type devices (MTDs) is one of the main driving force of 5G networks. In most of the current MTC systems, MTDs communicates directly with the eNodeB in one cell. This single-hop paradigm may not be able to support massive MTD where hundreds or thousands of MTDs attempt to set up communications. Furthermore, MTDs located at the boundary of a cell suffer from a high outage probability due to the interference from other MTDs. A costly solution is to deploy more eNodeBs and split the cell into multiple small cells. Instead of investing a huge amount of money on deploying extra eNodeBs or relays, cooperative communication has been demonstrated as an efficient and effective way to extend the coverage region and improve the throughput of cellular networks [25] [26] [27].

Conventionally, if an eNodeB fails to decode the packet, the MTD will retransmit the packet in the following available slot. However, it is with a high probability that the retransmission will fail again due to the correlated interference. In paper [28], the authors designed and analyzed a location-based cooperative strategy to improve the performance of massive MTC networks. One of the main idea of this paper is to select an inactive MTD acting as a relay for outage MTDs. Unlike

the work in [29] and [30] where the authors assumed the packet was known at the relay (base station) in prior, [28] considered the case where the relay has no prior information about the packet. To be specific, an inactive MTD is selected as a relay if it has successfully decoded the packet and if it is located within a circular area around the eNodeB. Otherwise, if there is no inactive MTD that can decode the packet, the source MTD will retransmit the packet. Both the simulation and numerical results demonstrate that spatiotemporal correlation of interference significantly affects the performance analysis of cooperative massive MTC networks and the designed cooperative strategy can significantly reduce the outage probability compared to conventional retransmission.

1.2 Proposed Research

Many of the CPS devices are expected to be in close proximity to each others. To provide a potential solution to the challenges mentioned in Section 1.1, D2D communication can allow CPS devices in close proximity to communicate directly with each other. For faster data collection, research efforts need to focus on preconfiguring the network faster using dynamic on-the-fly D2D connectivity and without the need for controllers or infrastructure deployment.

Relay-assisted D2D communications can help extend the limited communication range between CPS subnetworks [31], which in turn allows for a more efficient data collection. Therefore, in Chapter 3, we will analyze the spectral efficiency of the whole network if we offload machine-type communications (MTC) traffic on D2D links, where D2D relays will be equipped with RF energy harvesting to compensate for the need to use their own limited energy reserves to forward data for MTC devices. We will show that by doing so, we not only increase MTC spectral efficiency, but also we are able to achieve a balance and fairness in the weighted spectral efficiency among D2D and cellular users that are sharing the spectrum when there are enough number of available channels in the network and the D2D offloading factor is not set too high.

Moreover, in Chapter 4, we discuss about how to ease the spectrum access of CPS devices through D2D spatial spectrum sensing. Furthermore, we discuss about protecting these D2D links

from eavesdropping, since security is becoming a critical aspect in the cyber-physical space, especially with the large amount of traffic that is constantly flowing through the network.

Then, in Chapter 5, we investigate another potential solution for enabling CPS communications on cellular networks. To help relieve network congestion from CPS communications, we offload the latter from macrocells to small cells [32]. On the other hand, creating energy efficient solutions for the massive number of devices has always been a primary research focus by both academia and industry [33, 34, 35]. For instance, in [34], Wang et al. proposed an energy-efficient industrial IoT architecture consisting of sense entities (sensor nodes, smart devices) , RESTful service hosted networks to easily integrate heterogeneous devices, a cloud server and user applications. The proposed green architecture is carefully designed to extend network lifetime by reducing the energy consumption of sensing, processing and communication of the sense entities. Similar to Chapter 3, we take advantage of the advancements in renewable sources such as solar panels and wind turbines[1] i) to somehow offset the costs of SCBSs to serve offloaded CPS devices, and ii) to reduce carbon emissions for a greener environment. This would not be feasible to apply with macrocell BSs (MBSs) due to their larger energy consumption. Moreover, with extreme densification that is foreseen in future 5G networks [32], SCBSs will be irregularly located, with some being in remote areas where power grid is not feasible [36]. For these reasons, it makes sense to power SCBSs with energy harvesting.

Finally, in Chapter 6, we present a mobile-health CPS application as a case study, where we highlight the security aspect of the medical cyber-space. While cryptography can guarantee to some extent the data confidentiality, integrity and authentication [37], implementing it in CPS applications can be time consuming and costly in terms of computational overhead, high power consumption as well as the complexity of key management [38, 39]. For these reasons, we turn towards a lightweight low-complexity approach to protect the legitimate data from malicious attack by exploiting the physical characteristics of the wireless channels. This idea is not new as it dates back several centuries, where intentional echoes were generated by the circular shape of the Hall

[1] A solar panel of size 121 cm$\times$53.6 cm or a wind turbine with a rotor of 1 m in diameter under an 8 m/s wind speed can generate 100 W of electric power [36].

Pompeiana of Massimo in Italy in order to make its center indecipherable [40].

1.3 Research Impact and Contributions

By completing the above research tasks, the proposed research will be of value for the design and analysis of the current and emerging CPS communications. The proposed solutions will help facilitate the enabling and coexistence of CPS communications with current cellular networks.

- The novelty of this research lies in the ability to develop different solutions, schemes and systems of future 5G networks to help support the anticipated massive number of things. We expect that this research would provide great benefits to CPS by solving many of its challenges from connectivity to reliability to security.

- Furthermore, fundamental relationships between network performance and network parameters will be revealed, which will facilitate new systems design. What is more interesting is the possibility of applying many of these research results in various CPS applications.

- Tractable analytical solutions using stochastic geometry tools along with simulations using MATLAB software will allow the demonstration of the network performance, as well as the verification of the analysis for realistic network scenarios.

Chapter 2

Cyber-Physical Systems Meet Big Data: A Panoramic Overview

2.1 Introduction

In this chapter, we present CPS taxonomy. CPS requires cybersecurity to protect it against malicious attacks and unauthorized intrusion, which becomes a challenge with the enormous amount of data that is constantly flowing through the network. We provide an overview of the different security solutions proposed for CPS big data storage, access and analytics. Finally, we address CPS sustainability by surveying the different green solutions proposed in literature.

Before any processing or analysis, data needs to be acquired. The technological advancements in sensors have led to smarter, more efficient and low-cost sensors; the fact that facilitated their wide deployment. Two main sources to sense the data from: i) context-aware computing, and ii) social computing. With context-aware computing, data is sensed from physical sensors; virtual sensors which retrieve data using web services technology; logical sensors which combines both virtual and physical sensors such as gathering weather information; global sensors which collect data from middleware infrastructure; and remote sensors for earth sciences applications [41, 42]. As for social computing, participatory sensing and mobile crowd-sensing have led to shaping the

structure of social networks, in which users collect and share sensed data using their own smartphones rather than relying on sensors [43, 44, 45].

Cloud computing facilitates big data storage, processing and management in CPS, by breaking them down into workflows, which are then distributed over multiple dedicated servers. This allows CPS to provide pervasive sensing services beyond the capacities of individual things, in addition to lower latency and power consumption and larger scalability.

Once the data has been collected, making sense of it becomes one the most important aspects of CPS. However, it is important first to eliminate redundant information and reduce data complexity so useful information extraction can be efficiently performed. In this chapter, we will discuss about different tools to assist with the data mining process, mainly, feature selection, dimensionality reduction, knowledge discovery in databases, information visualization, computer vision, classification/clustering techniques, and real-time analysis.

After the data is transformed into manageable size, data mining tools (HDFS [46], MapReduce [47], R [48], S), real-time big data analytic tools (Storm [48, 49], Splunk [50]), and cloud-based big data analytic tools (GFS [51], BigTable [52], MapReduce) can be used to extract useful information and make sense of data, which would revolutionize the field of smart cities, environmental monitoring and others.

The ubiquitous cyber-physical world is susceptible to security threats to a large degree. These security vulnerabilities are made easier with the inability to effectively handle the large amount of data that is constantly flowing through the network; that, in addition to the lack of qualified security experts. Sensitive data stored in the cloud can be accessed or altered by unauthorized users. Cyber-security attacks on the computations, such as false data injection, can affect the integrity and accuracy of extracted results. For all these reasons, research efforts have been shifting towards proposing robust security solutions for big data CPS. In this chapter, we provide an overview of these proposed solutions.

In recent years, there has been a growing interest in green communications. Addressing green issues for CPS allows for a more sustainable and energy efficient system. Green solutions are

proposed for many aspects of CPS, mainly for i) data collection/storage such as minimizing the number of relay transmissions, removing redundant transmission links, and the use of data compression techniques; ii) CPS computing such as dynamic voltage and frequency scaling and traffic engineering techniques; iii) CPS processing such as designing energy-efficient orchestrators, checkpointing aided parallel execution (CAPE), reducing the amount of exchanged data between clouds, the use of cloudlets which are closer to users than distant clouds, among other solutions.

This chapter is organized into sections as follows: Section 2.2 describes the different sources and types of big data CPS, mainly context-aware computing and social computing, along with CPS-related big data applications. In Section 2.3, an overview of big data analytics techniques is provided. Section 2.4 provides a summary of the different security solutions proposed for CPS, mainly in storage, access and analysis. Section 2.5 addresses the sustainability and environmental concerns of CPS applications and the different green solutions proposed for CPS big data collection/storage, computing and processing. Finally, Section2.6 identifies CPS big data challenges and open issues. Conclusion remarks are presented in Section 2.7.

2.2 Sources and Types of Big Data for CPS

Several factors have driven the expansive use of sensors, mainly advancements in micro-electromechanical systems (MEMS) such as accessible design boards (Raspberry pi, Onion, Arduino) [53], and the new efficient hardware architectures and components, which made sensors more robust to hardware wearing from harsh environments. Moreover, many of these sensors incorporate accelerometers that are 1000x more powerful in terms of sensitivity than those used in a Nintendo Wii [54]. In this section, we discuss the different sensed big data sources and types by grouping them into social computing and context-aware computing. An illustration is provided in Fig 2.1.

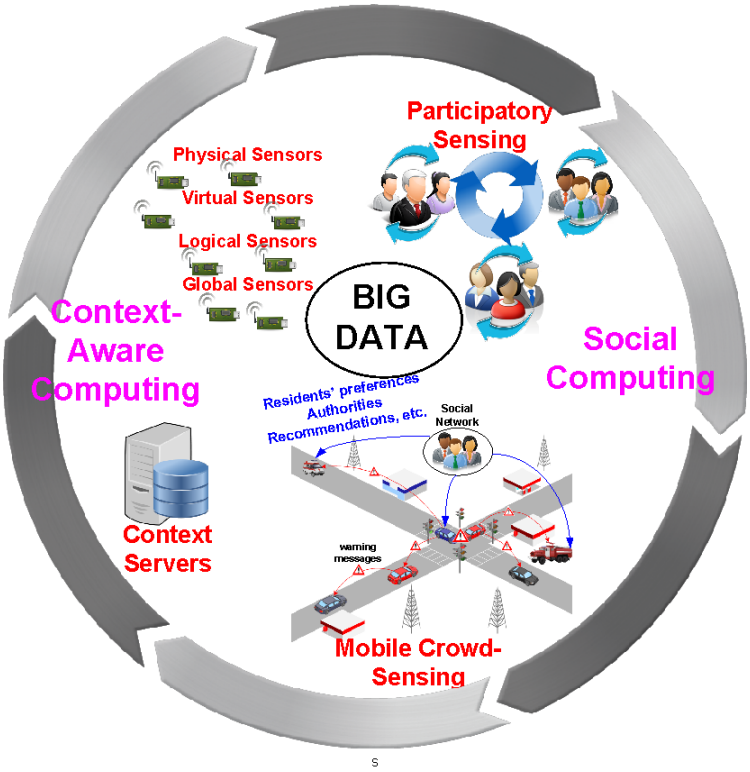

Figure 2.1: An illustration of the different CPS big data sources and types.

2.2.1 Context Aware Computing and Communications

The data that sensors collect for its specific application purposes is considered raw data, that is data that has been directly collected from the environment without further processing. With raw data alone, it becomes challenging to analyze and interpret it, let alone the big data generated by the large scale deployment of sensors. For data to provide relevant information that has meaningful value and easily interpretable, sensors need to engage in context-aware computing; that is, sensors need to store processed meaningful information, also known as "context information", that is easily understandable [55, 56]. An example to highlight the difference between raw sensor data and context information would be the blood sugar readings collected by bio-medical sensors on patient's body, which are considered raw data. When these readings are processed and represented as patient's average glucose level in the blood, they are referred to as context information. The quality of context (QoC) metric is used to assess the quality, validity, precision and up-to-dateness of context information [57]. Context-aware computing from acquisition, processing, storing and

reasoning, can be performed by the applications themselves, or by using libraries and toolkits, or even by using a middleware platform [41].

As for sources of context information, they can be retrieved directly from physical sensors, from virtual sensors (they collect data from different sources by using web services technology and represent it as sensor data), from logical sensors (a combination of physical and virtual sensors), from a middleware infrastructure (global sensor networks), from context servers (databases, web services), or even manually provided such as retrieving users' preferences.

The context information can be further classified into primary context and secondary context, which provides information on how the data was obtained. For example, reading RFID tags directly from different production parts in industrial plants is considered primary context, while obtaining the same information from the plant's database is referred to as secondary context [41, 58].

Remote sensing

Collecting sensor data of objects from a distance is referred to as remote sensing (RS) [59]. RS is an integral part of earth sciences. For instance, space-borne and airborne sensors collect multi-spatial and multi-temporal RS big data from the global atmosphere for purposes of earth observation and climate monitoring [60]. Other remote sensing applications include Google Earth that provides pictures of the earth's surface, weather reporting, traffic monitoring, hydrology and oceanography [61].

In [62], the authors proposed a big data analytical architecture for real-time RS data processing using earth observatory system. The real-time processing includes filtration, load balancing and parallel processing of the useful RS data. The RS datasets are normally geographically distributed across several data centers, leading to difficulties in loading, scheduling and transmission of data. That in addition to the high dimensionality of the RS data which makes their storage and data access rather complicated [60]. That is why in [63], Wang *et al.* proposed a wavelet transform to represent RS big data by decomposing the datasets into multiscale detail coefficients, which are estimated using expectation-maximization likelihood. In [64], the authors evaluate the quality of

RS data using statistical inference by using the prior knowledge of the dataset to get an unbiased estimator for the quality.

2.2.2 Social Computing

With the explosive increase in smartphones usage, mobile data has witnessed an unprecedented growth, carrying enormous amount of information on user applications, network performance data, service characteristics, geographic information, subscriber's profile, and so on [65]. This has led to shaping the notion of "mobile big data", which, unlike traditional big data in computer networks, has its own unique characteristics. One of these characteristics is the ability to partition mobile data in time and space domains, such as in minutes, hours, days, location, and so on. Furthermore, due to the features of smartphones' usage, the same traffic, on one hand, can be highly likely requested by a group of subscribers in certain time and location; and on the other hand, subscribers in close proximity may exhibit similar behavior and mobility patterns, all of which can help optimize network performance [66].

Social computing allows the integration of these social behaviors and contexts into web technologies to assist with predicting social dynamics, which can render the operation, planning and maintenance of social wireless networks easier than ever [67, 68]. For instance, due to high social correlations and relationships among subscribers, a user social network can be formed, in which the habit, interests, mobility, and sharing patterns can be used to construct social community structures and analyze communication behaviors. One such an example of user social application is the popular *Pokemon Go* game, where users in close proximity share real-time maps to hunt for Pokemon characters [66]. Another example where social computing can be beneficial is in emergency situations, such as the spread of infectious diseases, where taking the appropriate policies by analyzing human interactions and predicting the emergency's evolution can help protect the public health [67]. Next, we list two different social computing tools for data collection, mainly, participatory sensing and crowd-sensing.

2.2.2.1 Participatory sensing

Participatory sensing or community sensing allows users to collect and share information either within social groups (social sensing) or with everyone (public sensing) using their own smart devices [43, 44]. This means that sensors can be substituted by users for purpose of data collection, which can significantly reduce the monetary costs of deploying physical sensors. However, with participatory sensing comes several challenges such as the quality and trustworthiness of collected data, the willingness of participants to engage in the sensing tasks and protecting participants' personal information.

In [43], the authors proposed a participant coordination architecture that selects the most efficient participants without exposing participants' personal information to the application server. To protect participants' privacy, in [69], Chang *et al.* proposed a secure scheme called PURE which allows participants to reach the global model estimate via peer reviewing the local regression models. This enables participants to only report intermediate results back to the server without the need of sharing local private data with the server. In [70], Messaoud *et al.* proposed a mobile sensing scheme that reduces the sensing time required by participants, and increases the fairness of sensing tasks assignment to ensure participants' commitment to sensing while maintaining same data quality as in non-fair schemes. In an attempt to maximize the overall data quality, in [71], Wang *et al.* proposed a multi-task allocation framework (MTPS) which pays participants a compensation from a shared budget for each sensing task, with additional compensation if a participant is assigned more than one task. This greedy framework allows the allocation of multiple tasks to participants. In [72], participatory sensing for environmental data collection is used, where the urban resolution metric is used to measure the quality of urban sensing. In [73], participatory sensing is applied to vehicular networks, where location, speed, and fuel consumption of vehicles can be communicated to the server through phones aboard via a WiFi interface to reduce data transfer delay time.

2.2.2.2 Mobile crowd-sensing

Mobile crowd-sensing (MCS) can be considered as an extension to participatory sensing. In addition to collecting data from mobile devices (mobile sensing), MCS uses social sensing by integrating and fusing the contributed data from mobile devices with that of the mobile social network services in order to provide solutions to more complex queries [45]. In vehicular networks, with participatory sensing we can collect warning messages from vehicles to determine the traffic status. However, if in addition, a driver needs to know whether the route is safe to drive on based on authorities' recommendations, residents' preferences, etc., then MCS can be useful (see Fig. 2.1).

In [74], Xiang *et al.* uses MCS to construct accurate outdoor received signal strength (RSS) maps using error-prone smartphones. In [75], Wang *et al.* propose an energy-efficient cost-effective data uploading in MCS by providing incentives to participants to use the appropriate timing and network to upload the data. Data was offloaded to Bluetooth/WiFi gateways by using predictions on users' calls and mobility. To maintain relatively good performance of MCS applications, sufficient number of participants need to contribute to sensing. In [76], the authors discuss about the different incentives for MCS from entertainment, service and monetary incentives, in which participants can be recruited in multiple sensing tasks.

2.2.3 CPS Big Data Applications

We now present some of the main CPS big data applications in different fields: energy utilization, city management, and disaster events applications, along with a public safety case study model.

2.2.3.1 Smart Grids

Smart grids constitute an important aspect of sustainable energy utilization and are becoming more popular, especially with the advances in sensing and signal processing technologies. Automated smart decisions based on millions of data and control points play an important role in managing the energy usage patterns, understanding users' behaviors, reducing the need to build power plants,

and addressing supply fluctuations by using renewable resources [77]. That is why big data tools from cloud computing [77], mining and analytics [78, 79], performance optimization [80] and others have been dedicated for smart grids applications. Moreover, for reliable power grid, smart grids highly depend on cyber infrastructure. This poses several challenges such as exposing the physical operations of smart grid systems to cyber security attacks [81]. Furthermore, the collection of users' energy usage information such as the types of appliances they use, the eating/sleeping patterns, etc. can be very beneficial in optimizing smart grids' performance; however users' privacy can also be affected. In [82], Yassine *et al.* proposed a game theoretic mechanism to balance between users' private information and the beneficial uses of data.

2.2.3.2 Military Applications

Big data can also be exploited to improve experience, services, and training of military. Real-time authentication of command and control messages in cyber-physical infrastructures is of high importance for military services to ensure security. In [83], the authors develop a novel broadcast authentication scheme using special digital signatures for faster signature generation and verification, and packet loss tolerance. This can be useful to efficiently and rapidly secure military communications. In [84], the authors used Markov decision process to propose an approach to identify and reduce attacks' cost in military operations in order to protect important information through obtaining attack policies. Military satellite communications require to be resilient to ensure missions' success. This can be achieved using matrix-based protection assessment approach based on traditional risk analysis, where an attack can be assessed in terms of both ease of attack and impact of attack [85]. Mitigating the following five core threats allows the satellite communications to be free from weak vulnerabilities that can be easily exploited by attackers: waveform, RF access to enemy, foreign presence, physical access, and traffic concentration [85].

2.2.3.3 City Management

Big data can facilitate daily activities by using smart infrastructures and services. For instance, traffic patterns can be analyzed and routes can be computed to allow people to reach their destinations faster. In [86], the authors proposed to deploy road sensors to obtain information on the overall traffic, such as speed and location of individual vehicles. This information is then processed using graph algorithms by taking advantage of big data tools such as Giraph, Spark and Hadoop. This helps provide real-time intelligent decisions for smart efficient transportation. Safety systems, such as deploying surveillance systems, are another city management big data applications. A computer vision deep learning algorithm for human activity recognition was proposed in [87]. The model is capable of recognizing twelve types of human activities with high accuracy and without the need of prior knowledge, which makes it useful for security monitoring applications. Crowd detection and surveillance is another safety system big data application. A target individual needs to be easily inferred from visual information. In [88], the authors proposed such a framework that can easily detect target location and update the motion information to improve the detection.

2.2.3.4 Medical Applications

CPS health systems are foreseen to shape the future of tele-medicine in different areas such as cardiology, surgery, patients' health monitoring, which will significantly enhance the healthcare system by providing timely, efficient and effective medical decisions for a myriad of health applications such as diabetes management, blood pressure and heart rhythm monitoring, elderly support and so on [89]. With 774 million connected health-related devices [90] by 2020, a large volume of data from small-scale networks, such as e-health systems or mobile-health systems, needs to be stored, processed and analyzed to enable timely intervention and better management of patients' health.

With e-health systems becoming widely deployed in hospitals and health centers, research has been focused on efficiently deploying medical body area networks (MBANs) to reduce interference on medical bands from other devices [91]. In MBANs, biomedical sensors are placed in the

vicinity of patient's body or even inside her to sense health-related vital signals using short-range wireless technologies. The collected data is then multi-hopped to remote stations, so that medical staff can efficiently monitor patients' physiological conditions and disease progression [91]. For instance, in [92], elderly patients' health tracking application was proposed, where a mixed positioning algorithm allows for 24-hour monitoring of patients' activities and transmits an alarm to medical staff through SMS, e-mail or telephone in case of an abnormal event or emergency. However, transmitting this health information in a timely and energy-efficient manner is of utmost importance for e-health systems. In [93], a micro Subscription Management System (μSMS) middleware for e-health systems was presented. The μSMS platform allows sensor nodes to exchange information to provide event-driven services with dynamic memory and variable payload such as GPS coordinates, Home Context and so on. The designed architecture achieves lower memory overhead, lower software components load time and lower event propagation time than other similar proposals, which are all critical requirements for energy efficiency, reliability and scalability of e-health systems.

2.2.3.5 Disaster Events Applications

Network resilience and survivability are the utmost requirements for public safety networks. In case of a disaster or emergency event, the people who are first on scene are referred to as first responders, and they include law enforcement, firefighters, medical personnel and others [94]. Some of the major public safety requirements relate to the necessity of first responders to exchange information (voice and/or data) in a timely manner [94]. The big data can be used to support disaster events, such as analyzing big data from high resolution maps, floor plans and on-field video transmissions to transmit warning messages to authorities [95]. The remote sensing big data can be analyzed using a scalable hybrid parallelism approach to reduce the analytics execution time [96]. The large amount of data collected from previous earthquakes can be used to predict the future service availability areas, which can improve preparedness and response to such events [97]. A disaster domain-specific search engine can be constructed using big data to make the understanding

and preparedness of disaster attacks easier and faster for authorities [98].

2.3 Big Data Analytics

Big data analytics constitute one of the most important arenas in big data systems, as it allows to uncover hidden patterns, unknown correlations and other useful information, which in turn assist in boosting the revenues for many businesses. In this section, we present an overview of big data analytics tools and techniques.

2.3.1 Data Mining

One of the interesting features of CPS is the automated decision making. This means that CPS objects are supposed to be smart in sensing, identifying events and interacting with others [99]. The massive data collected by CPS needs to be converted into useful knowledge to uncover hidden patterns to find solutions, enhance system performance and quality of services. The process of extracting this useful information is referred to as data mining. One solution to facilitate the data mining process is to reduce data complexity by allowing objects to capture only the interesting data rather than all of it. Before data mining can be applied to the data, some processing steps need to be completed such as key features selection, preprocessing and transformation of data. Dimensionality reduction is one potential method to reduce the number of features of the data [100]. For instance, in [101], Chen *et al.* used neural network with k-means clustering via principal component analysis (PCA) to reduce the complexity and number of dimensions of gene expression data to extract disease-related information from gene expression profiles. Knowledge discovery in databases (KDD) is also used in different CPS scenarios to find hidden patterns and unknown correlations in data so that useful information can be converted into knowledge [102]. One such use of KDD is in smart infrastructures systems, where these systems need to answer queries and make recommendations about the system operation to the facility manager [103].

Tsai *et al.* [16] broke down the core operations of data mining into three main operations: data

scanning, rules construction and rules update. Data scanning is selecting the needed data by the operator. Rules construction includes creating candidate rules by using selection, construction and perturbation. Finally, candidate rules are checked by the operator, then evaluated to determine which ones will be kept for the next iteration. The process of scanning, construction and update operations is repeated until the termination criteria is met. This data mining framework works for deterministic mining algorithms such as k-means, and the metaheuristic algorithms such as simulated annealing and genetic algorithm.

Clustering, classification and frequent pattern are different mining techniques that can be used to make CPS smarter. Tsai *et al.* [16] discussed about two different purposes for clustering: i) clustering for infrastructure of IoT, and ii) clustering for services of IoT. Clustering for infrastructure of IoT helps enhance system performance in terms of identification, sensing and actuation, such as in [104], where nodes can exchange information between each other to identify whether they can be grouped together depending on the needs of the IoT applications. As for services of IoT, clustering can help provide higher quality services such as in smart homes [105]. On the other hand, classification does not require prior knowledge to complete the partitioning of objects into clusters, also known as unsupervised learning. Classification tools include decision trees, k-nearest neighbor, naive Bayesian classification, adaboost and support vector machines. Classification can also be done to improve infrastructure as well as services of IoT. Finally, frequent pattern mining is about uncovering interesting patterns such as which items will be purchased together with previously purchased items, or suggest items for customers to purchase based on customer's characteristics, behavior, purchase history, etc. Fig. 2.2 illustrates the CPS big data mining process for useful information extraction.

2.3.2 Real-time Analytics

Real-time analysis is another approach to produce useful information from massive raw data. Real-time streams data is first converted to a structured form before being analyzed by big data analysis tools such as Hadoop and MapReduce. Many application domains such as healthcare, transporta-

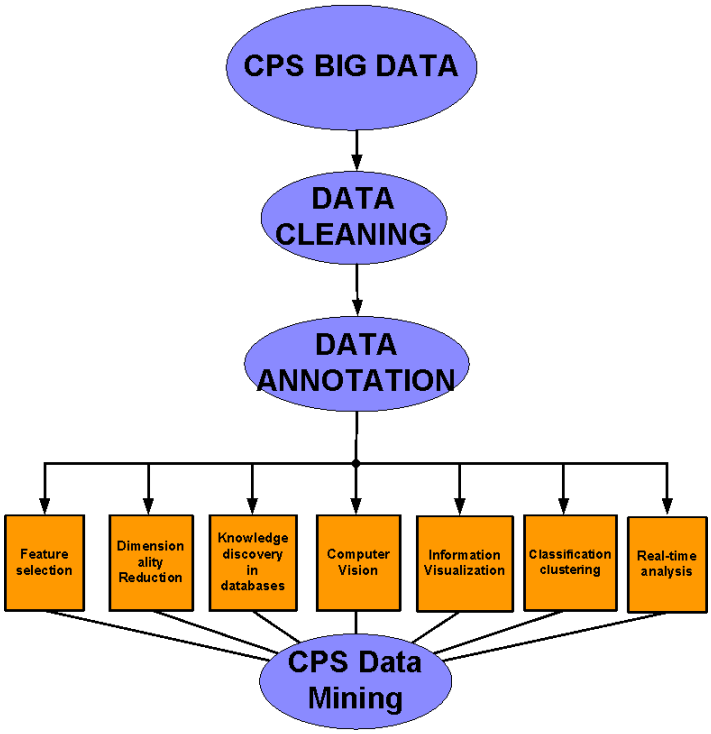

Figure 2.2: CPB big data mining process.

tion systems, environmental monitoring, and smart cities will require real-time decision making and control [44]. For example, Twitter data can be real-time analyzed to enhance the prediction process and to provide useful recommendations to users [106]; terrorist incidents data can be real-time analyzed to predict future incidents [107]; big data stream in healthcare can be analyzed to help medical staff make decisions in real-time, which can help save patients' lives and improve the healthcare services provided, while reducing medical costs [108]. Near real-time big data analysis architecture for vehicular networks was proposed in [109], which consists of a centralized data storage for data processing and a distributed data storage for streaming processed data in real-time analysis.

Arranging the data in a representative form can provide information visualization, which makes the information extraction and understanding of complex large-scale systems much easier [110]. In [111], the authors tackled the big data analytics in mobile cellular networks based on random matrix theory, where big data is represented in matrix form of size $n \times N$, where n is the number of data samples of a random vector x, and N is the number of independent realizations of x. For

cellular networks, big data manifests as big signaling data consisting of a large number of control messages to ensure reliability, security and efficiency of communications; big traffic data which require traffic monitoring and analysis to balance network load and optimize system performance; big location data generated by GPS sensors, Bluetooth, WiFi and so on, to assist in different areas such as transportation systems, public safety, crime hot spots analysis and so on; big radio waveforms data emanating from 5G massive MIMO systems to estimate users' moving speed for purposes of finding correlation among transmitted signals as well as assist in channel estimation; and finally big heterogeneous data such as data rate, packet drop, mobility and so on that can be analyzed to ensure cybersecurity.

Geographical information systems (GIS) is one important tool of visualization [112], as it can help real-time analysis of many applications such as in healthcare, urban and regional planning, transportation systems, emergency situations, public safety, and so on. In [112], the authors proposed a large-scale system data visualization architecture called X-SimViz, which allows users for real-time dynamic data analytics and visualization. Computer vision is another approach to detecting security anomalies. Visualization can also be useful tool in predicting real-time cyber attacks. For instance, in [113], the authors used computer vision to transform the network traffic data into images using a multivariate correlation analysis approach based on a dissimilarity measure called Earth Mover's Distance to help detect denial-of-service attacks. A computer vision deep learning algorithm for human activity recognition was proposed in [87]. The model is capable of recognizing twelve types of human activities with high accuracy and without the need of prior knowledge, which makes it useful for security monitoring applications.

2.3.3 Cloud-Based Big Data Analytics

Cloud-based analysis in CPS constitutes a scalable and reliable architecture to perform analytics operations on big data stream, such as extracting, aggregating and analyzing data of different granularities [114]. The massive amount of data is usually stored in spreadsheets or other applications, and a cloud-based analytics service, using statistical analysis and machine learning, helps reduce

the big data to a manageable size so information can be extracted, hypothesis can be tested, and conclusions can be drawn from non-numerical data such as photos. Data can be imported from the cloud and users are able to run cloud data analytics algorithms on big datasets, after which data can be stored back to the cloud [115]. For instance, in [116], the authors used cloud computing using MapReduce algorithm to conduct analysis on crime rates in the city of Austin using different attributes like crime type and location to help build a design that prevents future crimes for public safety.

Even though cloud computing is an attractive analytics tool for big data applications; however it comes with several challenges, mainly concerning security, privacy and data ownership, which will be discussed further in Section 2.4. In [11], the authors extended the use of clouds to mobile cloud computing to help overcome the challenge of resources limitations such as memory, battery life and CPU power. A mobile cloud computing architecture was suggested for healthcare applications with discussion on various big data analytic tools available. In [117], the authors suggested using a hybrid cloud computing consisting of public and private clouds to accelerate the analysis of massive data workloads on MapReduce framework without requiring significant modifications to the framework. In a private cloud, cloud services delivered over the physical infrastructure are exclusively dedicated to the tenant. The hybrid cloud uses a set of virtual machines run on the private cloud, which take advantage of data locality, and another set of virtual machines run on a public cloud to run the analysis at a faster rate.

To optimize the utilization of cloud computing resources, predicting the expected workload and the amount of resources needed becomes important to reduce waste. In [118], the authors developed a system that predicts the resources requirements of a MapReduce application to optimize bandwidth allocation to the application; whereas in [119], the authors used linear networks along with linear regression to predict the future need of new resources and VMs. When the system fails short in predicting the right amount of resources needed, it becomes incapable of accommodating a high workload demand, leading to anomalies. Anomalies detection is an essential part of big data analytics, as it helps improve the quality of service by checking if the measurements of

the workload observed and the baseline workloads diverge by a specific margin, where the baseline workloads provide a measure on how the demand changes during a period of time based on historical records [120].

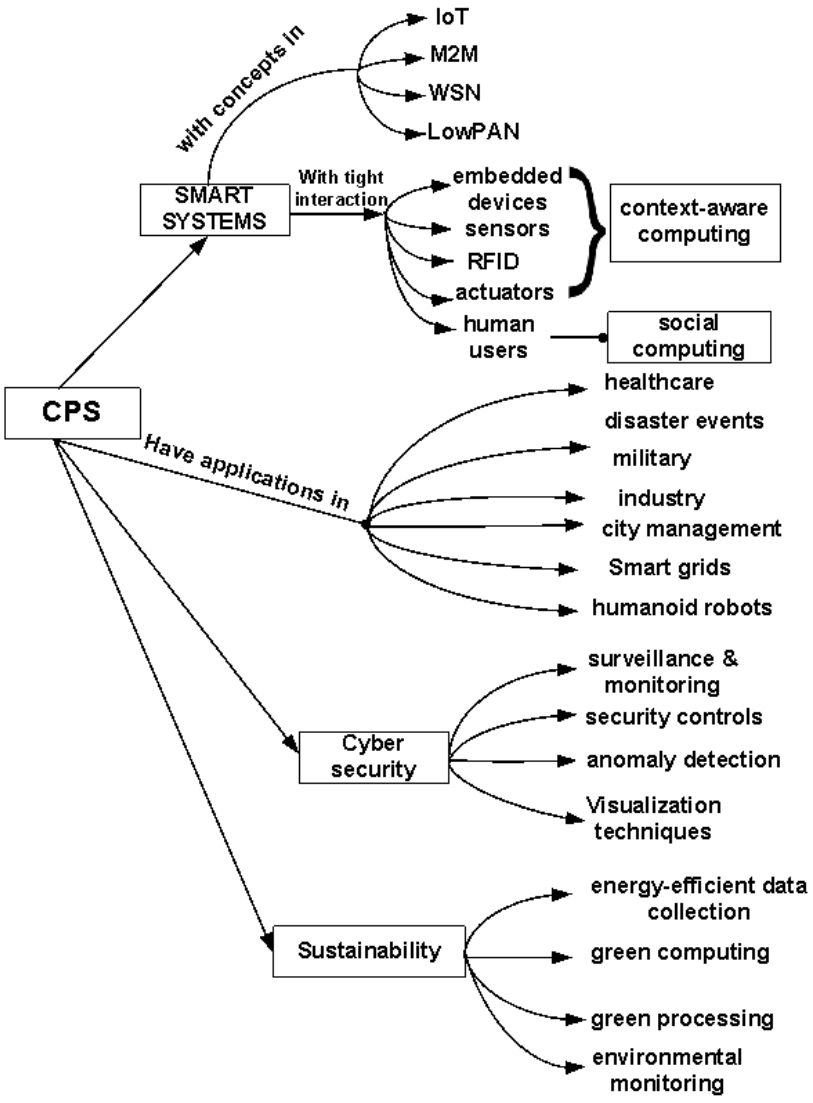

Figure 2.3: An illustration of CPS taxonomy.

2.4 Big Data Cybersecurity and Privacy

In the realm of cyber physical systems, the tight interaction among physical objects which collect and transmit large volume of data place security threats under the spotlight of attention. With

this enormous amount of data that is constantly flowing through the network, it becomes essential to protect the system from cyber attacks. In this section, we provide an overview of the different security solutions proposed for big data storage, access and analytics (see Table 2.1 for a summary).

2.4.1 Security in Big Data Storage and Access

While data storage in the cloud offers several advantages in terms of data storage, availability, scalability and processing, it increases the chance of malicious attacks, that in addition to potential privacy invasion by cloud operators who can have access to sensitive data. All this puts a question mark whether cloud data storage is feasible, especially for governmental agencies and financial industries. Several works have attempted to solve the security challenges of cloud storage. For instance, Gai *et al.* proposed a method that splits files into encrypted parts and store them in distributed cloud servers without users' data being directly reached by cloud service operators [121]. In [122], the authors optimized the data placement on cloud servers that minimizes retrieval time of data files while guaranteeing their security based on the distance between nodes that store the data chunks, such that the malicious attacker cannot guess the locations of all the data chunks. In [123], the authors suggested that data to be encrypted and decrypted before sending it to clouds. When data needs to be transferred from one cloud to another, data privacy and integrity become important. In [124], Ni *et al.* proposed a secure data transfer scheme where users encrypt the data blocks before uploading to the cloud. When transferring from one cloud to another, a security protocol was described using secret keys and a signature checking with polynomial-based authentication was performed without retrieving data from the source cloud. While the mentioned works considered encryption as a way to protect the data from privacy violations, encryption introduces a new challenge: cloud data deduplication, especially when data is shared among many users. Even though deduplication can save up to 95% in terms of needed storage for backup applications [125], and 68% for standard file systems [126]; however it wastes resources, consumes energy and makes the data management very complicated. In [127], Yan *et al.* attempted to solve the deduplication problems by proposing a scheme, where the users upload the encrypted data to the cloud along

with a token for data duplication check, which is then used by the cloud service providers to check whether the data has already been stored. A scheme to verify data ownership was presented to ensure secure data management.

2.4.2 Security in Big Data Analytics

Enabling security and privacy aspects of big data analytics have attracted a great attention from the scientific community, mainly due to different reasons. First, the data is more likely to be stored, processed and analyzed in several cloud centers leading to security issues due to the random location of data. Second, big data analytics treat sensitive data in similar way to other data without taking security measures such as encryption or blind processing into consideration [128]. Third, big data computations need to be protected from malicious attacks in order to preserve the integrity of the extracted results. In the realm of CPS, the enormous amount of data makes the monitoring of security-related information for anomaly detection a challenging task for analysts; that, in addition to the lack of qualified security experts. In healthcare, for instance, security of information extraction from massive amount of data and accurate analytics are of high importance. Sensitive data recorded in databases need to be protected by monitoring which applications and users get access to the data [129]. In order to guarantee a strong secure big data analytics, the following tasks can be performed [130]:

- Surveillance and monitoring of real-time data streams
- Implementation of advanced security controls such as additional authentication and blocking suspicious transactions
- Anomaly detection in behavior, usage, access and network traffic
- Ability to defend the system against malicious attacks in real-time
- Adoption of visualization techniques that give a full overview of network problems and progress in real-time.

Machine learning, among other tools, offers a promising solution to automate many of the above mentioned security-related tasks, especially with the continuous growth of the flowing data in terms of scale and complexity. Through the process of training datasets, machine learning makes possible the detection of future security anomalies by detecting unusual activities in the network traffic. To achieve a higher accuracy, a large volume of training datasets are needed; however this would be at the cost of added overhead and storage constraints. The process of training can be supervised, unsupervised or semi-supervised, depending on whether the outcome of a particular dataset is already known. In specific, the system starts by classifying similar datasets into clusters to determine their anomaly. A human analyst can then explore and identify any unusual data. The outcome found by the analyst can then be fed back to the training system in order to make it more "supervised" [131]. This has the potential of helping the training system adapt to new forms of threats without human intervention, so actions can be immediately taken before actual damages occur. Different approaches for anomaly detection exist in literature such as discretizing the continuous domain into different dimensions such as in the surveillance system in [132], where the author partitioned the surveillance area into a square grid where the positions and velocities of the moving objects falling in each cell are modeled by a Poisson point process. Another approach is the multivariate Gaussian analysis in which data is flagged as abnormal when it lies a number of standard deviations away from the mean. For instance, in [133], the authors used multivariate Gaussian analysis to detect internet attacks and intrusions by analyzing the statistical properties of the IP traffic captured. In clustering methods such as k-means clustering, data points can be grouped into clusters based on their distance to the center of the cluster. Then, if the data point lies outside of the group cluster, it is considered as an anomaly. The authors in [134] used kernel k-means clustering with local-neighborhood information to detect a change in an image by optimally computing the kernel weights of the image features such as intensity and texture features. As for the artificial neural network approach, one implementation of such a model is the autoencoder, also known as replicator neural network, which flags anomalies based on calculations of the difference between the test data and the reconstructed one. This means that if the error between test and

reconstructed data exceeds a specified threshold, then it is considered far away from a healthy system distribution [135]. An example of such approach is given in [136], where the authors used the autoencoder as a high accurate low-latency model to detect anomalies in the energy consumption and operation of smart meters.

Table 2.1: A summary table of security solutions proposed for CPS

Literature	Security Solutions
[121], [122], [137]	Secure data placement on cloud
[113], [131], [133], [134], [135], [136], [138], [139], [140], [141] , [142], [143]	Anomaly detection
[121], [123], [124], [127], [144], [145]	Cryptographic solutions
[69], [129], [143],[146]	Advanced security controls
[87], [88], [113], [132], [134], [147]	Visualization techniques

2.5 Big Data Meet Green Challenges for CPS

Greening big data systems allows to address sustainable and environmental concerns. In this section, we provide a panoramic discussion on the different green solutions for CPS big data collection/storage, computing and processing. Fig 2.4 shows different sustainable applications, along with challenges and solutions for a greener CPS.

2.5.1 Energy-Efficient Data Collection

With massive number of interacting objects, gathering sensed data poses a challenge in terms of energy consumption, mainly due to the limited communication range between subnetworks, necessitating that objects act as relays for surrounding objects in order to extend their communications. This affects the lifetime of objects since each object needs to relay large volume of data generated by its neighbors [148]. In this context, different solutions have been proposed for different big data applications. In [148], Takaishi *et al.* proposed energy efficient solutions for data collection in densely distributed sensor networks. In an attempt to reduce the number of relay transmissions

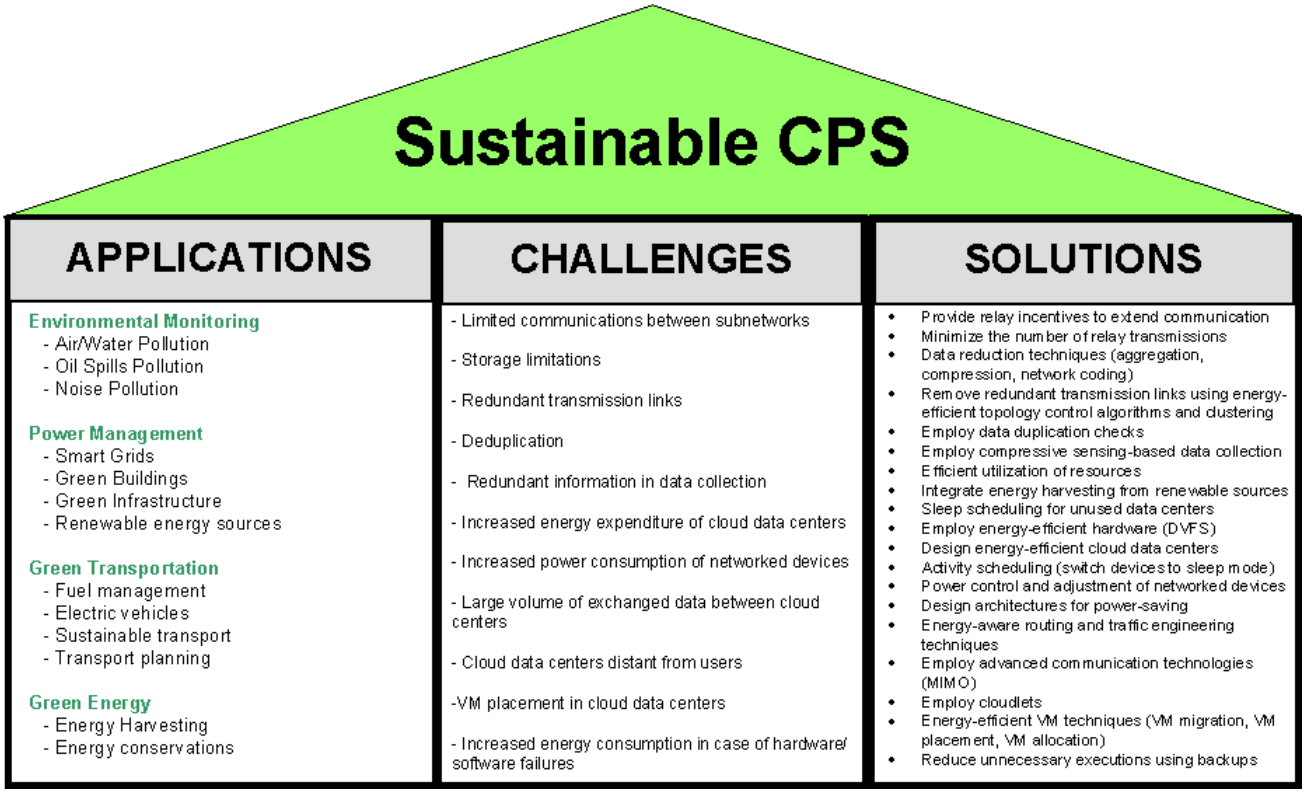

Figure 2.4: Sustainable CPS: applications, challenges and solutions.

needed, sensor nodes transmit their data to a data collector node, the sink node, when they become close in proximity to it. Therefore, it becomes important to figure out the trajectory that the sink node needs to follow based on nodes' information such as location and residual energy, as well as the cluster formation in order to reduce the energy consumption of data collection. Data compression technology is another solution to help deal with challenges of data storage, collection, transmission, processing, and analysis. For instance, in [149], the authors proposed a highly efficient lossy data compression based on smart meters' load features, states and events with a small reconstruction error. ZIP-IO compression technique was proposed in [150] using FPGA as a potential implementation framework. Video compression is another important tool in big data for surveillance applications. The authors in [151] proposed a background-based coding optimization algorithm that uses the residual gradient and the block edge differences to improve picture quality while achieving high level of compression.

Removing redundant transmission links can also reduce energy consumption while increasing

network capacity. Topology control algorithms such as local minimum spanning tree (LMST) [152] and Local Tree-based Reliable Topology (LTRT) [153] have low computational complexity and can help obtain the best logical topology which can be beneficial for energy efficient data collection. In addition to removing redundant transmission links, removing redundant data can help save energy, such as in [154], where a compressive-sensing-based collection framework was proposed for reducing data redundancy and saving energy. To implement this solution, an online learning module predicts the amount of data (principal data) that needs to be collected for compressive sensing. This means the principal data is supposed to represent the whole big data using the compressive sensing technique. Then, each node can locally tweak the collection strategy dynamically depending on neighbors status, residual energy, and link quality. Nodes' clustering can also contribute to energy saving by reducing the number of data collection and transmissions, such as fan-shaped clustering proposed in [155] for large-scale networks with energy efficient selection of a cluster head and relay node. Other clustering algorithms exist in literature, such as the well-known Low-Energy Adaptive Clustering Hierarchy (LEACH) [156], which can be useful for big data wireless sensor networks.

2.5.2 Green Computing

While cloud centers are becoming an important aspect of big data computing to process data chunks in parallel, they contribute to a high energy expenditure, leading to increased costs and maintenance [157]. Therefore, research efforts are shifting towards creating sustainable big data computing techniques.

Shojafar *et al.* proposed a job scheduler between servers called MMGreen to reduce energy consumption of computing in cloud data centers [158]. The MMGreen architecture is composed of physical servers hosting VMs connected to a front-end component that manages the incoming workload. Scheduler jobs that use dynamic voltage and frequency scaling (DVFS) technique for energy efficient servers include static scheduler whose power consumption is independent of clock rates and usage, and sequential schedulers which attempt to minimize reconfiguration costs by per-

forming offline resource provisioning via predicting future workload information [159]. In [158], the authors described different techniques to reduce energy consumption such as DVFS to reduce VMs' frequencies and real-time adjustment of VMs frequencies processing and switching while maintaining quality of service to users. In [160, 161], M2M power savings were optimized by reducing the execution frequency of some activities without negatively impacting the human-to-human communications.

Besides targeting the energy efficiency of cloud servers, network devices also need energy efficient solutions since they also contribute to the total energy expenditure of the cloud data center. Traffic engineering is one solution for this problem, which takes advantage of the traffic prediction to turn off network devices such as switches during idle periods in order to reduce power consumption [162, 163, 164, 165]. Traffic engineering techniques, such as the software defined networking (SDN)-based traffic engineering [166], allow the network devices to dynamically adapt to current workload. One problem with traffic engineering techniques is that the predicted traffic pattern might not be accurate due to the variability of big data applications running in the data center. This makes the network configuration suffer from frequent oscillations, since it needs to be updated frequently leading to performance degradation [167]. To take into consideration this time-varying aggregate traffic load, one proposed solution is to include flow deadlines to measure the speed at which requests' responses are delivered to users. This allows the design of energy-efficient scheduling and routing for data center networks [167, 168, 169]. Another solution to enhance the inaccurate traffic engineering techniques is to take into consideration the unique features of data centers such as regularity of the topology, VM assignment, application characteristics. Such a framework was proposed in [170], where the energy-saving problem was solved in two steps: i) a VM assignment algorithm that integrates application characteristics and network topology to better understand traffic patterns for energy efficient routing, and ii) an algorithm that minimizes the number of switches and balances traffic flow among them. Experimental results showed a 50% energy savings using the proposed framework.

2.5.3 Green Processing

An energy-efficient orchestrator for smart grid applications was proposed in [171]. The green orchestrator coordinates sustainability between smart grids and big data enterprises from green infrastructure (data centers) to running green frameworks such as Hadoop MapReduce. The orchestrator's main components are: i) a green lesser to establish a per-job service-level agreements (SLA) that takes into account the available power, the power consumption statistics of jobs, the network and server states; ii) a pre-execution analyzer that executes jobs based on their power consumption statistics; iii) a network and server states predictors; iv) a network traffic analyzer which helps eliminate redundant traffic using traffic engineering techniques; v) a VMizer that intelligently places VMs such that some nodes are put to sleep; (vi) a pizer that schedules and places processes to a subset of clusters such that system resources are efficiently utilized; and (vii) a post-execution analyzer to analyze the energy profile of completed jobs.

Another green big data processing architecture is checkpointing aided parallel execution (CAPE), which uses checkpoints that save the sates of processes to avoid restarting unnecessary executions from beginning in case of hardware or software failures [172, 173, 174]. CAPE also allows threads of a shared-memory program to be executed in parallel on a distributed memory architecture rather than a shared memory architecture. The CAPE architecture can lead to energy saving since if the execution period of processors is short, they can go to idle mode rather than staying active for the whole execution of the program. This makes it beneficial in processing big data in CPS applications [174, 175].

Another approach to green big data processing is the efficient utilization of network resources by reducing the volume of communications that need to be exchanged in cloud data center networks. For instance, Asad *et al.* proposed spate coding for the purpose of reducing the amount of exchanged data, but without compromising the rate of information exchange [176]. Spate coding incorporates both index coding and network coding, and uses side information originating from several processes sharing a physical node to encode packets. This coding technique was shown to reduce the volume of communications by 62%, along with other advantages such as improv-

ing the utilization of system resources from disk utilization, queue size, and the number of bits transmitted during shuffle phase of Hadoop (200%) [176]. Other approaches to reduce the burden on data centers from the information exchange include traffic flow prediction to reduce network transfers [118, 177], and redundancy elimination scheme to remove redundant information data exchange, among others [178, 179, 180].

2.5.4 CPS-based Green Big Data Toward Green Applications

CPS-based big data applications can contribute to greening different sectors: environment, economic, and social/technical issues [35, 181, 33]. As for the environment, efforts are made to reduce air/water pollution as well as the impact of climate changes. For instance, sensors can be deployed to monitor air and water qualities. Using MapReduce or Spark programming frameworks, the concentration of pollutants can be monitored and studied [182]; the air quality not covered by monitoring stations can be estimated [183], and the causalities of air pollutants can be identified using urban big data dynamics [184]. Pollution can also originate from oil spills. Predicting such catastrophes very early can help save beaches, coastlines and waters [35, 181]. Marine oil spills can be detected using a large archive of remote sensing big data [42]; and a real-time warning can be generated from a quantitative data analysis using supervised oil system [185]. Concerning water pollution, underwater sensors can be deployed to monitor water environment, such as water level, water flow, temperature, and pressure. The sensor network can be connected to a cloud platform via a wireless transceiver for analysis and visualization [186]. Noise pollution in cities is another contributing factor to environmental pollution, which can have negative impact on health, especially with the increasing number of circulating vehicles [35, 181]. Noise pollution levels can be predicted by collecting four data sources: complaint data, social media, points of interests, and road network data [187]. These data can be gathered by deploying static municipal sensors, together with participatory sensing with smart phones in order to provide more accurate noise maps [188].

As for green economics, CPS applications can be targeted for optimizing the energy use. One

example is FirstFuel, which monitors temperature and lightnings inside buildings by checking the running status of the equipments, such as fans, heating and cooling units [35]. Power management can be realized using sensors monitoring the whole building, as well as using smart meters for electricity consumption measurements. Energy efficient smart meters solution has been proposed in [189] using coalition game that maximizes the pay-off values of smart meters. An approach to predict daily electricity consumption inside buildings using data analysis was proposed in [190]. The authors used canonical variate analysis to group electricity consumption profiles into clusters in order to identify abnormal energy usage. Energy efficiency can also be employed in transportation systems to reduce fuel wastage. One example is [191], where the authors used electric vehicles (EV) battery model to estimate the driver's behaviors and driving range to improve energy efficiency. Social media and participatory sensing can also be used toward greener environment. For instance, in [192], the authors used social media to optimize smart grid management. In [193], participatory sensing was used to implement a navigation service called GreenGPS to allow drivers to obtain customized routes that are the most fuel-efficient.

2.6 Big Data Challenges and Open Issues for CPS

While ongoing research is focusing on CPS enterprise development and applications, effective solutions to combat security flaws have not received the attention they deserve, which places question marks on the foreseen integration of CPS in critical infrastructures. This matter is made worse with CPS devices having i) limited computational capabilities to employ data confidentiality, privacy preservation and authentication; ii) the semi- or fully-autonomous security management (mutual authentication, key arrangement, etc.) [194]; and iii) the high computational overhead cost of cryptographic solutions [195]. Low-complexity and lightweight ciphers such as PRESENT [196] have been developed; however research efforts should go beyond cryptography, especially that such solutions can be time consuming and costly in terms of high power consumption as well as the complexity of key management [38, 39].

Correctness of CPS is another research area under the spotlight of attention. Due to dynamic nature of physical environment, CPS need to constantly adapt to new situations while operating and functioning properly with little or no human supervision [197]. The use of models can allow the early detection of failures by simulating different components of complex designs to verify the integration of the whole system [198, 199]. CPS components verification to ensure they are working properly or that they meet execution time requirements is another approach to ensure correctness [200, 201, 202]. Future research shall focus on creating robust real-time anomaly detection and correctness techniques that have low overhead and implementation costs.

For faster data collection, research efforts need to shift towards devices that do not need to preconfigure to a network with dynamic on-the-fly D2D connectivity, and without the need of controllers or infrastructure deployment. Furthermore, to extend the communication range among devices, incentivized devices with tokens will replace dedicated relays. In terms of CPS computing, research directions should shift towards faster data processing by moving data processing closer to the sources and by speeding-up big data handling. For a faster and efficient CPS analysis, research activities need to be further conducted on information fusion techniques, especially that information originates from heterogeneous devices with varying capabilities. By perfecting the fusion algorithms, related information can be aggregated for analysis leading to higher quality information [203].

2.7 Conclusion

The emerging idea of CPS is made easier with the technological advancements in big data processing and analysis. When combined with artificial intelligence, machine learning, and neuromorphic computing techniques, CPS will bring about new applications, services and opportunities, all envisioned to be automated with little or no human intervention. This will help revolutionize the "smart planet" concept, where smarter water management, smarter healthcare, smarter transportation, smarter energy, and smarter food will create a radical shift in our lives.

Chapter 3

Energy Harvesting-Based D2D-Assisted Machine-Type Communications

3.1 Introduction

Supporting massive numbers of machine-type communication (MTC) devices poses several challenges for future 5G networks including network control, scheduling, and powering these devices as discussed in Chapter 1. A potential solution is to offload MTC traffic onto device-to-device (D2D) communication links to better manage radio resources and reduce MTC devices' energy consumption. However, this approach requires D2D users to use their own limited energy to relay MTC traffic, which may be undesirable.

This motivates us to exploit recent advancements in RF energy harvesting for powering D2D relay transmissions. In this chapter, we consider a D2D communication as an underlay to the cellular network, where D2D users access a fraction of the spectrum occupied by cellular users. This underlay model presents a fundamental trade-off: to protect cellular users, the spectrum available to D2D users needs to be reduced, which limits the number of D2D transmissions, but increases the amount of time that D2D users can spend harvesting energy to support MTC traffic. We first introduce the concept of spatial RF energy harvesting, where D2D users harvest RF power from

uplink cellular transmissions, if it exceeds a predesigned threshold, in a spatial region. Using tools from stochastic geometry, we obtain a closed form expression for the probability of activating RF power conversion circuit by making full use of spatial locations of ambient RF signals. Subsequently, we study the impact of RF energy harvesting region radius to harvest sufficient power on the signal-to-interference (SIR) ratio of D2D network. Simulation results provide insights for the required advancements to design highly efficient RF harvesting circuits.

Then, we characterize the spectral efficiency of MTC, D2D and cellular users using stochastic geometry in order to determine the optimal spectrum partition factor that achieves fairness and balance in the network, while increasing the average MTC spectral efficiency.

Table 3.1: List of Key Notations

Notation	Definition
Φ_k	PPP with $k = \{\text{B,U,D,C,M}\}$ for macro BSs, UEs, D2D users, cellular users, and MTC devices respectively.
λ_k	Intensity of PPP with $k = \{\text{B,U,D,C,M}\}$ for macro BSs, UEs, D2D users, cellular users, and MTC devices, respectively.
R_{B}	Radius of a macrocell.
P_k	Transmit power with $k = \{\text{D,C,M}\}$ for D2D users, cellular users, and MTC devices respectively.
θ_k	Signal-to-interference-plus-noise ratio (SINR) target threshold with $k = \{\text{D,C,M}\}$ for D2D users, cellular users, and MTC devices respectively.
$\lvert B\rvert$	Total number of available channels.
κ	The spectrum partitioning factor, i.e., the fraction of spectrum available to D2D users.
$\gamma_{i,j}$	SINR between node i and node j.
R_{r}	Radius of relay assist region.
N_{r}	Number of relay users in the assist region.
α	Path-loss exponent of cellular, D2D and MTC transmissions.
ρ	Transmission probability of D2D users.

3.2 Fundamentals of Spatial RF Energy Harvesting for D2D Cellular Networks

3.2.1 Introduction

D2D communications have recently grown in popularity due to their powerful benefits, many of which have been validated in scientific literature. D2D communication allows users in close proximity to communicate directly with each other bypassing the base station (BS). This helps offload part of the organic cellular traffic to D2D networks, thereby improving spectral utilization, increasing capacity, decreasing delay, improving cellular coverage, and increasing energy efficiency. All these benefits make D2D communications especially suitable for social networking applications such as wireless video streaming, media sharing, etc. However, D2D communication brings with it several challenges such as cross-tier interference from D2D transmissions, power control, spectrum sharing, peer discovery, and a myriad of other challenges that, fortunately, are being addressed by the scientific community.

Energy efficiency is one of the many challenges that arises as the world prepares to move towards 5G. With high data rates, which are expected to be 1000x more than 4G, energy efficiency will need to improve by about the same amount [32]. Energy harvesting will be one of the important areas that will help increase energy efficiency to maintain the power consumption. More specific, energy harvesting from ambient RF signals will be among the forefront technologies to power small devices. As a matter of fact, 3.5 mW harvested power was achieved at a distance of 0.6 meters and 1 uW at a distance of 11 meters using Powercast RF energy-harvester operating at 915 MHz [204]. Future advancements in RF circuitry will bring about more harvested power for small low-power devices.

RF energy harvesting was considered in [205] for cognitive radio networks. An RF power conversion circuit extracts DC power from the received RF signals. This RF power conversion circuit is activated only when the received RF power in the RF energy harvesting zone around an

access point (AP) is greater than a predesigned threshold, which depends on circuit sensitivity. However, the authors in [205] did not characterize the probability of harvesting RF energy in terms of the spatial locations of ambient RF signals. In addition, the impact of RF energy harvesting on the network's performance was not analyzed.

Similar to [205], in [206], an energy harvesting region was considered for relay users, where they harvest ambient RF energy from access points in order to improve the communication reliability of D2D users. By considering energy harvesting, the authors derived the distribution of relays that increase the D2D transmission opportunities. Unlike our work, they did not characterize the spatial energy harvesting rate and they did not consider the effects of spatio-temporal correlated interference. Finally, in [207], an energy harvesting model for IoT devices that does not require battery storage nor voltage converter was proposed. A test-bed implementation of the harvesting system showed an 8% increase in the amount of harvested power and 60% increase in device lifetime.

It should be noted that we are only considering energy harvesting for D2D users rather than cellular users, since the former require much less power to communicate over short distances, especially with the short payload of MTC traffic; hence the current advancements in RF energy harvesting technology [208] can be very useful for D2D users. Moreover, emerging D2D applications are usually data-hungry social networking applications such as wireless video streaming, media sharing, etc [209]. These applications generally consume more energy, where the RF harvested energy can offset some of the additional energy consumption of these applications.

In this section, we obtain a closed form expression of the probability of activating RF power conversion circuit, and then we analyze, through simulations, several parameters such as cellular users' intensity, which impact the amount of harvested power. The results will help advance the design of efficient RF energy harvesting circuits.

We assume that users cannot use the same channels for harvesting ambient RF energy and transmitting information simultaneously, a valid assumption for small low-complex devices. Furthermore, we only consider energy harvesting for D2D users, especially with the increasing energy

demands of D2D social networking applications. We summarize the contributions of this section as follows:

- First, to the best of our knowledge, this is the first work to analyze the impact of RF energy harvesting region on the D2D network performance. Using tools from stochastic geometry, we analytically characterize the probability of activating RF power conversion circuit by making full use of spatial locations of cellular RF signals.

- Second, we carry out simulations to study the impact of RF energy harvesting zone radius, the spectrum partition factor, the total number of channels, and the intensity of cellular users on the D2D network performance.

- Third, our simulation results provide insights on the required RF harvesting radius to harvest minimum required power for transmission. This provides the required advancements to design highly efficient RF harvesting circuits.

The remainder of this Section is organized as follows. In Section 3.2.2, a system model for D2D network underlaid with cellular network is presented. Section 3.2.4 introduces the RF energy harvesting technology and model, while Section 3.2.5 presents the performance analysis of spatial RF energy harvesting technique. Section 3.2.6 presents the simulations and analytical results. Finally, conclusions are drawn in Section 3.2.7.

3.2.2 System Model

3.2.3 D2D Network Model

Fig. 3.1 shows an example of a hybrid network that consists of D2D and cellular user equipments (UEs) with spatial RF energy harvesting. We consider an uplink cellular network, where D2D users and cellular users (CU) share the licensed spectrum. By using an uplink channel, the D2D transmitters experience less interference when compared to using the downlink, due to the lower

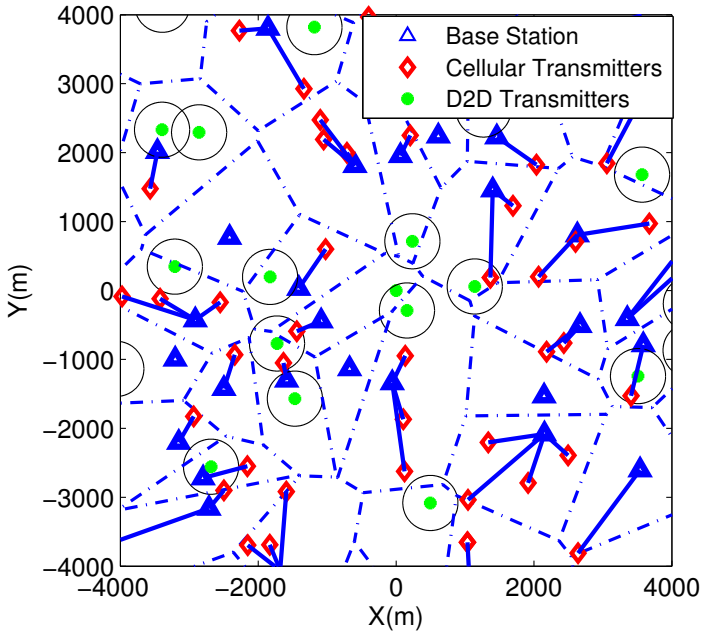

Figure 3.1: A realization of a hybrid network consisting of D2D and cellular links with spatial RF energy harvesting with the circles representing the RF energy harvesting zones.

transmit power of cellular users when compared to that of the BS. Considering the in-band underlay system model, D2D transmitters randomly access the spectrum that may be occupied by cellular users. Compared to overlay model where D2D users and cellular users use orthogonal in-band spectrum, the underlay model can achieve higher throughput since the spectrum is more efficiently reused [1] (see Fig. 3.2). The locations of the macro BSs are modeled by a homogeneous Poisson point process (PPP), Φ_B with intensity λ_B. Let $\mathscr{A}_c(k,R_B)$ denotes the coverage region of a macrocell, approximated by a disk with radius $R_B = (\pi\lambda_B)^{-1/2}$ centered at a generic BS k. The circle approximation can help simplify the problem formulation by reducing the number of variables that are needed to represent the system while having a comparable performance to the spatial locations in the entire plane [210]. UEs are uniformly distributed in the coverage region of the corresponding BS and form a homogeneous PPP, Φ_U with intensity λ_U [211].

Types of Nodes: We differentiate between two different types of nodes δ_i with $i = D,C$, for D2D user and cellular user, respectively.

- **D2D user:** Here, a D2D user can either be a D2D transmitter or a D2D receiver. The UEs in

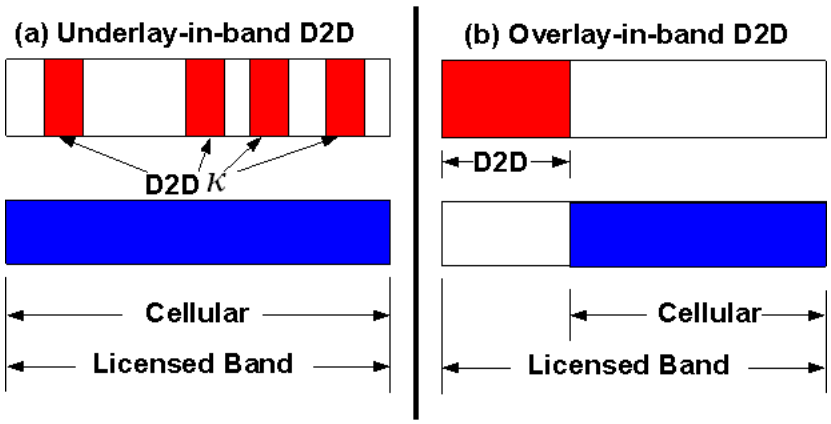

Figure 3.2: Different D2D spectrum sharing scenarios [1].

D2D mode form a thinning PPP Φ_D from Φ_U, with intensity $\lambda_D = \mathscr{P}(\delta_i = \delta_D)\lambda_U$. A UE i is in D2D mode if the end-to-end signal-to-interference-plus-noise (SINR) ratio between transmitter and receiver is greater than θ_D.

- **Cellular user:** The UEs in cellular mode form a thinning PPP Φ_C from Φ_U, with intensity $\lambda_C = \mathscr{P}(\delta_i = \delta_C)\lambda_U$. Note that $\Phi_U = \Phi_C \cup \Phi_D$, and $\Phi_D \cap \Phi_C = \emptyset$.

We assume that each D2D receiver is uniformly distributed with probability density function (PDF) [212]:

$$f_{\mathrm{D}}(r) = \frac{2r}{\mu^2},\ 0 \leq r \leq \mu, \tag{3.1}$$

where μ is the maximum allowable distance between a D2D pair. In this chapter, we assume that all users use constant transmit powers, and we leave channel inversion power control for Chapter 4. Denoting by $|B|$[1] the number of channels; D2D transmitters can access $\kappa|B|$ of them randomly, where $\kappa \in [0,1]$ measures the fraction of spectrum available to D2D users [1]. The D2D transmit power P_D is split among the $\kappa|B|$ subchannels as $\hat{P}_D = (1/(\kappa|B|))P_D$.

Let us denote the channel SINR between nodes i and j by $\gamma_{i,j}$. Accordingly, the probability that a source node s is in D2D mode is given by: $\mathscr{P}(\delta_s = \delta_D) = \mathscr{P}\left(\gamma_{s,d} \geq \theta_D\right)$, with $\gamma_{s,d}$ denoting the channel SINR between source node s and destination node d. If a source node s cannot be in D2D mode, then it becomes a cellular node, such that $\mathscr{P}(\delta_s = \delta_C) = 1 - \mathscr{P}(\delta_s = \delta_D)$.

[1] $|.|$ denotes the set cardinality.

The distance between any two nodes i and j is denoted by $\|i-j\|$. We assume that the power of the signal transmitted by UEs decays at a rate of $l(i,j) = \|i-j\|^{-\alpha}$, where $\alpha > 2$ is the path-loss exponent of both cellular and D2D transmitters. Rayleigh fading with mean one is used to model the small-scale fading over each channel, with $h_{i,j}$ denoting the channel coefficient between nodes i and j.

Let ρ be the probability that a BS assigns any $\kappa|B|$ channels to serve its users. Then ρ is given by [213]:

$$\rho = 1 - \sum_{n=0}^{(1-\kappa)|B|} \mathscr{P}(N_{\mathrm{u}} = n), \tag{3.2}$$

where N_{u} is the number of users associated to a BS, and $\mathscr{P}(N_{\mathrm{u}} = n)$ is given in [Eq. (6) in [213]]. Then, $\tilde{\Phi}_{\mathrm{C}}$ is a point process representing the set of CUs not using $\kappa|B|$ subchannels with intensity $\tilde{\lambda}_{\mathrm{C}} = (1-\rho)\lambda_{\mathrm{C}}$. Note that $\tilde{\Phi}_{\mathrm{C}}$ is not a PPP due to the correlation among uplink CUs, where each CU is assigned a unique channel by the BS. However this dependency is weak and can be ignored as shown in [214, 211] in order to provide a tractable analysis.

3.2.4 Spatial RF Energy Harvesting

3.2.4.1 RF Energy Harvesting Technology

In RF energy harvesting, radio signals with frequencies ranging from 3 kHz to 300 GHz can be used as a medium to carry energy in the form of electromagnetic radiation. The received signal strength of an RF transmission decays at a rate that is inversely proportional to the distance between the transmitter and receiver, specifically at 20 dB per decade of the distance [215]. Thus, RF energy harvesting depends on three main factors: the transmit power of the energy source, the distance between the RF energy source and the harvesting node, and the wavelength of the RF signals [216].

In the context of energy harvesting, RF sources can be classified into two categories: dedicated RF sources and ambient RF sources. Dedicated RF sources use license-free ISM frequency bands to provide energy to nodes when a more predictable energy supply is needed. The downside of dedicated RF sources is that they can incur a high cost for deployment in the network, and their

power can be limited by federal regulations due to health and safety concerns about RF radiation. For example, in the 900 MHz frequency band, the maximum allowable transmission power is 4 W, which gets attenuated to 10 uW at a moderate distance of 20 m [215].

On the other hand, ambient RF sources provide "free" energy because they are not intended specifically for RF energy transfer. The transmit power can vary from 10^6 W for TV towers to around 0.1 W for mobile communication devices and WiFi systems [215]. As a matter of fact, an antenna of 300 mm $\times$ 300 mm was used to power embedded sensors from ambient digital TV signals, where the net harvested RF energy reached 126.2 uW [217]. Furthermore, in a recent breakthrough, *Drayson Technologies* has developed a new RF energy harvesting technology called "Freevolt" which harvests energy from wireless data and broadcast networks. The expected harvested RF power achieved was 100 uW at an RF power density of 40 uW/cm^2 using a patch antenna. This would be very useful for D2D users and MTC devices since they operate at lower power than cellular users. More details on this technology can be found in [208].

Although RF energy harvesting has the least energy intensity compared to other energy harvesting sources, it has several desirable properties. In particular, it does not depend on the weather or geographical region (unlike solar and wind energy); it can be used in any location that has a high incidence of strong ambient RF waves; and it can drive more than one device at the same time. In this paper, we assume that D2D transmitters harvest energy from ambient interference caused by uplink cellular transmissions.

3.2.4.2 Spatial RF Energy Harvesting Model

Each D2D UE is equipped with an RF power conversion circuit that extracts DC power from the received electromagnetic waves [218]. Because the RF circuit has sensitivity requirements, it requires an input power larger than a predesigned threshold in order to activate it [205]. Thus, we define an RF energy harvesting zone as a disk with radius R_h centered at each D2D user $x \in \Phi_D$, denoted as $\mathscr{A}_h(x_i, R_h)$ as shown in Fig. 3.1, where x_i is the spatial location of D2D user i. The amount of harvested RF power depends greatly on the number of cellular interferers inside the RF

harvesting zone, and thus on the harvesting radius R_h. Due to their low transmit power, we neglect the power harvested from other D2D transmitters. This motivates us to introduce the concept of *Spatial RF Energy Harvesting* for D2D cellular networks, where the received power inside the spatial region $\mathscr{A}_h$ allows the D2D user to harvest RF power. In what follows, We characterize the probability of activating RF circuit.

Assume the D2D transmitter is located at the origin, we are interested in a state $\mathscr{S}$, where there is at least one cellular transmitter inside $\mathscr{A}_h$ in order to harvest RF power from. It is important to note that we are only interested in cellular transmitters that are not using $\kappa|B|$ subchannels, since D2D users cannot use $\kappa|B|$ subchannels for harvesting energy and transmitting information simultaneously to simplify the system operation and analysis. That is, when a cellular transmitter and a D2D transmitter are using the same channel, the latter cannot harvest energy. We define state $\mathscr{S}$ as:

$$\mathscr{S}: y[n] = \sum_{\substack{i \in \tilde{\phi}_C \cap \mathscr{A}_h \\ \tilde{\Phi}_C \cap \mathscr{A}_h \neq \emptyset}} \left(P_C h_{i,0} l(i,0)\right)[n] + z[n], \tag{3.3}$$

where $n = 0, 1, ..., N-1$ is the sample index with N being the total number of samples; $\left(P_C h_{i,0} l(i,0)\right)[n]$ is the nth sample of the received signal from cellular transmitter i by a typical D2D user; $z[n]$ is the Gaussian noise ($z[n] \sim \mathscr{N}(0, \sigma_n^2)$); and $\tilde{\phi}_C$ is a realization of $\tilde{\Phi}_C$ denoting the set of cellular transmitters' locations. Each D2D user tests the average received power using the test statistics ξ, which is expressed as $\xi = 1/N \sum_{n=0}^{N-1} y[n]$. Let ε denotes the energy harvesting threshold to activate the RF power conversion circuit. Denote the probability of activating RF power conversion circuit as $p_t = \mathscr{P}\{\xi > \varepsilon | \mathscr{S}\}$. When N is large, by central limit theorem, the distribution of ξ approaches Gaussian distribution. Thus, we can characterize the mean and variance of ξ under $\mathscr{S}$ as [219]:

$$\begin{aligned} \mathrm{E}(\xi) &= \sum_{i \in \tilde{\phi}_C, |\mathscr{A}_h| > 0} P_C h_{i,0} l(i,0) = I_{\mathrm{RF}}, \\ Var(\xi) &= \frac{1}{N^2} \left(I_{\mathrm{RF}} + \sigma_n^2\right), \end{aligned} \tag{3.4}$$

where $|\mathscr{A}_h|$ denotes the number of cellular transmitters inside the RF harvesting zone. As can be seen in Eq. (3.4), the random variable I_{RF} depends on the spatial distribution of cellular users. Because the amount of harvested RF power in the harvesting zone depends heavily on I_{RF} (and thus on state $\mathscr{S}$), we can express the probability of activating RF power conversion circuit p_t as:

$$p_t = \int_0^{\infty} f_{I_{\mathrm{RF}}}(x)\, \mathscr{P}\left(\xi > \varepsilon | \mathscr{S}, I_{\mathrm{RF}}\right) dx, \tag{3.5}$$

where $f_{I_{\mathrm{RF}}}(x)$ is the PDF of I_{RF}; and $\mathscr{P}\left(\xi > \varepsilon | \mathscr{S}, I_{\mathrm{RF}}\right) = Q\left(\frac{N(\varepsilon - x)}{\sqrt{x+\sigma_n^2}}\right)$, where Q-function is the tail probability of the standard normal distribution.

3.2.5 Performance of Spatial RF Energy Harvesting

In this section, we obtain an expression for $f_{I_{\mathrm{RF}}}(x)$ in order to characterize p_t. The following lemma provides an expression of the Laplace transform of I_{RF} using stochastic geometry tools.

Lemma 1.

$$\mathscr{L}_{I_{RF}}(s) = \frac{\exp\left(-\frac{2\tilde{\lambda}_C \pi^2 (s)^{2/\alpha} P_C^{2/\alpha}}{\alpha \sin(2\pi/\alpha)}\right) - \mathscr{L}_{I_0}(s) e^{-\tilde{\lambda}_C \pi R_h^2}}{1 - e^{-\tilde{\lambda}_C \pi R_h^2}}, \tag{3.6}$$

where $\mathscr{L}_{I_0}(s) = \exp\left(-\frac{2\pi\lambda_B P_C s}{(\alpha-2)R_h^{\alpha-2}} {}_2F_1\left(1, 1-\frac{2}{\alpha}; 2-\frac{2}{\alpha}; -\frac{sP_C}{R_h^{\alpha}}\right)\right)$;
${}_2F_1\left(a,b;c,z\right) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-tz)^{-a} dt$ *is the hypergeometric function.*

Proof : *See Appendix 8.1.*

As can be seen from Lemma 1, the distribution of I_{RF} depends on RF energy harvesting zone radius R_h. For the special case of $\alpha = 4$, the Laplace transforms of I_{RF} becomes:

$$\mathscr{L}_{I_{\mathrm{RF}}}(s) = \frac{\exp\left(-\frac{\tilde{\lambda}_C \pi^2 \sqrt{sP_C}}{2}\right) - \mathscr{L}_{I_0}(s) e^{-\tilde{\lambda}_C \pi R_h^2}}{1 - e^{-\tilde{\lambda}_C \pi R_h^2}}, \tag{3.7}$$

with

$$\mathscr{L}_{I_0}(s) = \exp\left(-R_B^{-2}\sqrt{sP_C}\arctan\left(\frac{\sqrt{sP_C}}{R_h^2}\right)\right). \tag{3.8}$$

The following lemma provides an expression for the PDF of I_{RF} for $\alpha = 4$ using the inverse Laplace transform.

Lemma 2.

$$\begin{aligned} f_{I_{RF}}(x) &= \frac{\mathscr{L}^{-1}\left(e^{-\frac{\pi^2\tilde{\lambda}_C}{2}\sqrt{sP_C}}\right) - e^{-\tilde{\lambda}_C\pi R_h^2}\mathscr{L}^{-1}\left(\mathscr{L}_{I_0}(s)\right)}{1-e^{-\tilde{\lambda}_C\pi R_h^2}} \\ &= \frac{\pi^{3/2}\sqrt{P_C}\tilde{\lambda}_C}{4\left(1-e^{-\tilde{\lambda}_C\pi R_h^2}\right)}x^{-3/2}\exp\left(-\frac{\pi^4\tilde{\lambda}_C^2 P_C}{16x}\right) - \frac{e^{-\tilde{\lambda}_C\pi R_h^2}}{1-e^{-\tilde{\lambda}_C\pi R_h^2}}f_{I_0}(x), \end{aligned} \tag{3.9}$$

with the PDF of I_0 can be accurately approximated as an inverse Gaussian distribution [220] as: $f_{I_0}(x) \approx \sqrt{\frac{\vartheta}{2\pi x^3}}\exp\left(\frac{-\vartheta(x-\upsilon)^2}{2\upsilon^2 x}\right)$, *where* $\vartheta = (3P_C)/(2R_B^2P_C^2)$ *and* $\upsilon = P_C/(R_h^2R_B^2)$.

Theorem 1. *The probability of activating the RF power conversion circuit, when the path loss exponent* $\alpha = 4$*:*

$$\begin{aligned} p_t = &\frac{\pi^{3/2}\sqrt{P_C}\tilde{\lambda}_C}{4\left(1-e^{-\tilde{\lambda}_C\pi R_h^2}\right)}\int_0^\infty Q\left(\frac{N(\varepsilon-x)}{\sqrt{x+\sigma_n^2}}\right)x^{-3/2}e^{-\frac{\pi^4\tilde{\lambda}_C^2P_C}{16x}}dx \\ &- \frac{e^{-\tilde{\lambda}_C\pi R_h^2}}{1-e^{-\tilde{\lambda}_C\pi R_h^2}}\int_0^\infty Q\left(\frac{N(\varepsilon-x)}{\sqrt{x+\sigma_n^2}}\right)f_{I_0}(x)dx. \end{aligned} \tag{3.10}$$

Proof : *The result is obtained by substituting (3.9) into (3.5).*

Remarks: It is interesting to note that the expression of p_t takes into account not only the energy harvesting threshold ε, but also the network density, noise power and the RF harvesting zone radius R_h. In what follows we demonstrate the impact of the RF harvesting radius R_h on the amount of harvested RF power. Remember that R_h is determined by the energy harvesting circuit sensitivity for a given received power. When the RF harvesting zone is small ($R_h \to 0$) due to

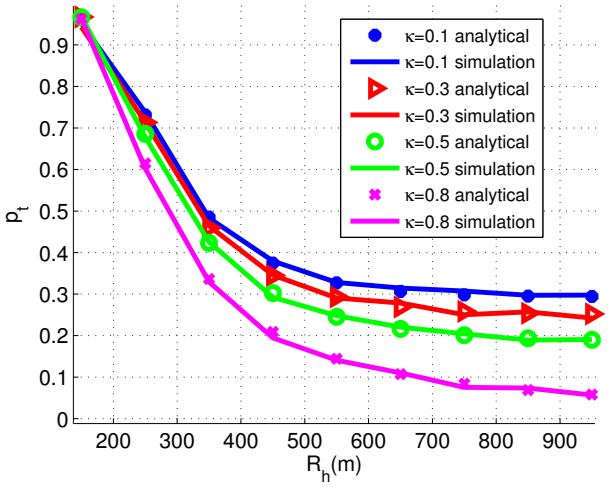

Figure 3.3: The probability of activating RF power conversion circuitry in terms of R_h for different values of κ ($\theta_D = 10$ dB).

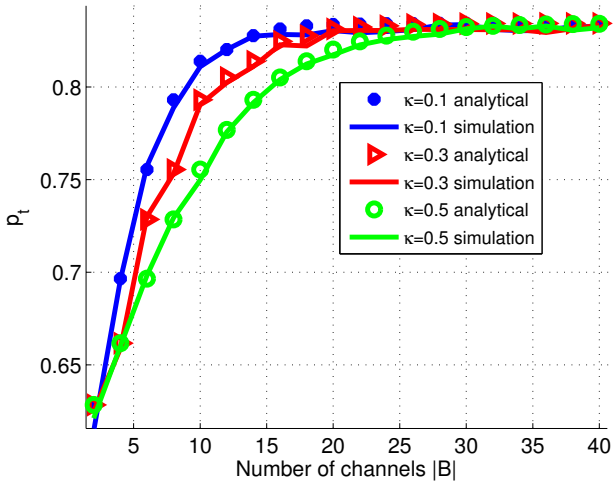

Figure 3.4: The probability of activating RF power conversion circuitry versus $|B|$ for different values of κ ($\lambda_D = 20\lambda_B$; κ =0.5; θ_D =10 dB).

low energy harvesting circuit sensitivity, $p_t \to 1$ (remember that p_t is conditioned on having at least one cellular transmitter inside $\mathscr{A}_h$). This is explained by the fact that if there is at least one cellular transmitter inside a very small $\mathscr{A}_h$, then the received interference power from the cellular transmitter to D2D user will be large enough to activate the RF power conversion circuit. However, as $R_h \to \infty$, we can express p_t^{∞} as:

$$p_t^{\infty} = \frac{\pi^{3/2}\sqrt{P_C}\tilde{\lambda}_C}{4} \int_0^{\infty} Q\left(\frac{N(\varepsilon - x)}{\sqrt{x+\sigma_n^2}}\right) x^{-3/2} e^{-\frac{\pi^4 \tilde{\lambda}_C^2 P_C}{16x}} dx. \tag{3.11}$$

Let $P_{\text{req}} = \hat{P}_D$ denotes the minimum required transmit power for D2D users. Then, the probability p_h of harvesting at least P_{req} is given by Eq. (3.10) with $\varepsilon = P_{\text{req}}$.

3.2.6 Simulation Results and Analysis

In this section, we present Monte Carlo simulation and analytical results to analyze the spatial RF energy harvesting model for D2D cellular networks. Unless otherwise stated, we set the following system parameters: R_B = 788 m (which corresponds of an inter-BS distance of 1500 meters), N =

5000, P_C = 200 mW, $\hat{P}_D$ = 2 mW, μ = 90 m, $\alpha = 4$, $\lambda_B = 1/\left(\pi R_B^2\right)$, $\lambda_U = 10\lambda_B$ and $|B| = 10$.

Fig. 3.3 shows the probability of activating RF power conversion circuit, p_t, in terms of the energy harvesting zone, R_h, for several values of the spectrum partition factor, κ, for comparison. First, as R_h increases, p_t decreases as explained by the remarks of Theorem 1. What is interesting to see is that as κ increases, more D2D transmitters are accessing the spectrum, which in turn decreases the intensity of cellular users not using $\kappa|B|$ subchannels, $\tilde{\lambda}_C$, thereby reducing the probability of harvesting RF power.

Fig. 3.4 depicts the behavior of p_t in terms of the total number of available channels $|B|$, for several values of κ. As $|B|$ increases, so does p_t. This can be explained by the fact that with more available channels, more cellular transmissions occur, which means D2D users can harvest more RF energy. Furthermore, we note that beyond $|B| = 15$, not much improvement in terms of p_t is seen, and that is due to the increased interference from cellular users to D2D users which is compensated by an increase in lifetime of D2D users. We can see that as κ increases, p_t decreases.

3.2.7 Conclusions

In this section, we analytically characterized the probability of activating RF energy harvesting circuit for D2D users by making full use of spatial locations of cellular transmitters. Results have revealed insights on designing highly efficient RF energy harvesting circuits by analyzing the impact of the RF harvesting zone radius, the spectrum partition factor, the total number of channels, and the intensity of cellular users on the D2D network performance.

3.3 D2D-Assisted Machine-Type Communications

Now that we have derived and analyzed the spatial RF energy harvesting for D2D users, we will use it to somehow offset the costs of D2D relays using their own limited energy to forward data for MTC devices.

When combining the spectrum partition factor with D2D-assisted MTC communication based

on RF energy harvesting, we face a fundamental trade-off: reducing the spectrum partition factor to protect cellular users from underlaid D2D transmissions reduces the probability that UEs operate in D2D mode [1], but increases the amount of time that UEs can spend harvesting energy to support relaying MTC traffic. Therefore, the spectrum partition factor should be set small enough to simultaneously manage interference to cellular users and to ensure that UEs harvest sufficient energy for relaying, but not so small that too few UEs operate in D2D mode to realize the benefits of D2D-assisted MTC communication. The objective of this paper is to study this trade-off analytically using tools from stochastic geometry.

We summarize the contributions of this section as follows:

- First, to the best of our knowledge, this is the first work to analyze the spectral efficiency of energy-harvesting based D2D-assisted MTC communication by taking into consideration the correlation in the interference at D2D relay and destination nodes. This provides a more accurate characterization of system performance than existing work [221]. Furthermore, this is the first work to analyze the impact of RF energy harvesting on the spectral efficiency of MTC, D2D and cellular networks. Using tools from stochastic geometry, we obtain an analytical expression of the expected RF energy harvesting rate by making full use of spatial locations of cellular transmitters. Then, we obtain the average energy utilization rate by defining a transmission region for a D2D user. Finally, we characterize the average transmission probability of a D2D transmitter in terms of the expected energy harvesting rate and the average energy utilization rate.

- Second, we provide a tractable analytical framework for statistical analysis of D2D-assisted MTC communications underlaying cellular networks by characterizing the spectral efficiency of MTC, D2D and cellular networks.

- Third, the analytical framework allows us to highlight the gains achieved by offloading MTC traffic on D2D links, when compared to a system without any assistance from D2D communications. This would be extremely useful in future 5G networks where the support of mas-

sive MTC devices is important. In addition, our simulation results provide insights on the trade-off between increasing D2D transmission probability by harvesting more RF energy and the cellular spectral efficiency.

The remainder of this section is organized as follows. In Section 3.3.1, a system model for a D2D-assisted MTC network underlaid with a cellular network is presented. Section 3.3.2 characterizes the expected RF energy harvesting rate, the energy utilization rate as well as the transmission probability of a D2D user. Section 3.3.3 presents the spectral efficiency analysis of cellular, D2D and MTC networks. Section 3.3.4 presents the simulations and analytical results. Finally, conclusions are drawn in Section 3.3.5.

3.3.1 D2D-Assisted MTC System Model

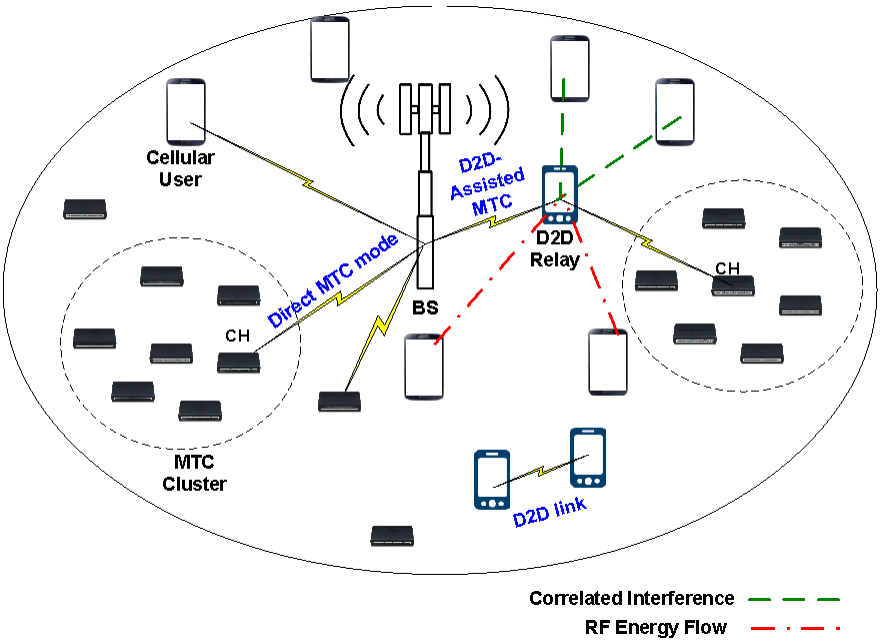

Figure 3.5: An example of a hybrid network with D2D-assisted MTC and cellular links with RF energy harvesting.

Fig. 3.5 shows an example of a hybrid network that consists of cellular transmissions, D2D transmissions, and D2D relaying with RF energy harvesting, along with MTC devices (smart sensors, actuators, meters, etc.) grouped into clusters. Again, we consider D2D communication as

an underlay to the uplink cellular network, such that D2D users and cellular users (CU) share the licensed uplink spectrum, while MTC devices use orthogonal spectrum resources. In this section, we consider both conventional D2D transmissions between two UEs and relaying D2D transmissions for MTC traffic. Different MTC applications have different data traffic characteristics. For instance, smart metering applications are characterized by low rate, infrequent and small data transmission, whereas surveillance applications are characterized by high rate, frequent and large blocks data transmission. This makes it essential to group MTC devices into clusters based on their common features, functionality and applications to make their operation and management easier for the operator. Cluster members send their data to a cluster head (CH), which collects all the data in a single packet and transmits it to the BS either directly or through a nearby D2D user. Offloading MTC on D2D links provides an efficient way to use radio resources, in addition to reducing the transmission power due to using intra-cluster communications and short range D2D links [222]. We re-denote $\mathscr{A}(k, R_{\mathrm{B}})$ as the coverage region of a macrocell, approximated by a disk with radius R_{B} centered at a generic BS k [211]. In what follows, we refer to cellular and D2D users as UEs. UEs are modeled by an independent HPPP, Φ_{U}, with intensity λ_{U}, while MTC devices are modeled by an independent HPPP, Φ_{M}, with intensity λ_{M}.

Mode selection: Two operational modes are suggested for UEs: 1) cellular mode and 2) potential D2D mode. A potential D2D user is a user with D2D traffic which can either use the cellular or the D2D mode for communications based on one or a combination of different selection criteria. This means that a potential D2D user can switch between D2D and conventional cellular communications. In this paper, we use signal-to-interference-plus-noise ratio (SINR) threshold-based mode selection and we conduct our analysis on a fixed topology that remains the same for long period of time before changing (semi-static model), since the mode selection depends on the traffic generated in the network, which is very challenging and costly to obtain [1]. In what follows, we assume that mode selection has already been completed and thus we define the two different types of UEs in the network. Furthermore, we assume that MTC clustering has already been performed

and we proceed with the performance analysis[2].

In this work, we assume that D2D users are willing to act as relays for MTC traffic as long as they have harvested enough energy to cover the cost of relaying. Thus, relays rely on "free" harvested energy when assisting MTC devices, rather than their own energy reserves. While this effectively "compensates" users for serving as relays, it does not necessarily provide users incentives to relay. For example, a selfish user would still prefer to keep the harvested energy for herself, rather than use it to relay data for MTC. We note that providing incentives to prevent this type of selfish behavior is out of the scope of this paper; however, in our prior work, we have investigated this problem for relay-assisted base station-to-device (B2D) communication (see [224]). Furthermore, we assume that D2D users are trustworthy to relay MTC traffic; however in reality that might not be true since D2D users can be malicious or dishonest. This means that D2D users might attempt to modify MTC packets or decide not to transmit them for selfish purposes such as conserving their battery energy. Note that in [225], the authors have investigated this topic by proposing a secure multi-hop device-to-device communication protocol to transport IoT traffic to the corresponding servers over the Internet where D2D users share secret keys to enable secure data forwarding. Note that D2D links are not just used for relaying MTC traffic, but they are also used in the conventional context to allow two UEs to communicate directly with each other.

In addition to D2D user and cellular user, we define an MTC device as follows:

MTC device: MTC CH (MTCCH) can use two different modes for transmission of the collected packet from its cluster members as follows:

- *D2D-assisted MTC mode:* There is a D2D relay available in the vicinity of the MTCCH, and the end-to-end SINR using a D2D relay is greater than a target threshold θ_{M}.

- *Direct MTC mode:* There is no available D2D relay to provide services to the MTCCH; however the end-to-end SINR ratio of the direct link between MTCCH and the BS is greater than θ_{M}. Note that if this condition holds and there are available D2D relays, then by default, the CH will choose to go through the relay to save energy.

[2]Clustering schemes for MTC have been thoroughly studied in the literature such as [223].

Fig. 3.6 shows the topology of a D2D-assisted MTC link. We assume that distance D_Y between the MTCCH and the BS is uniformly distributed with probability density function (PDF):

$$f_{\mathrm{D}_Y}(\mathrm{d}_y) = \frac{2\mathrm{d}_y}{\mu_{\mathrm{m}}^2},\ 0 \le \mathrm{d}_y \le \mu_{\mathrm{m}}, \tag{3.12}$$

where μ_{m} is the maximum allowable distance between an MTCCH and the BS. We define an assist region for an MTCCH i located at x_i as $\mathscr{A}_{\mathrm{r}}(x_i, R_{\mathrm{r}})$, which is a disk centered around the MTCCH i with a radius R_{r}. The MTCCH selects the closest D2D relay in $\mathscr{A}_{\mathrm{r}}(x_i, R_{\mathrm{r}})$. Therefore, the relays are randomly and independently located inside this disk with isotropic direction and Rayleigh distributed distance with PDF:

$$f_{\mathrm{D}_X}(\mathrm{d}_x) = \frac{2\pi\lambda_{\mathrm{D}}}{1 - e^{-\pi\lambda_{\mathrm{D}}R_{\mathrm{r}}^2}}\mathrm{d}_x e^{-\lambda_{\mathrm{D}}\pi\mathrm{d}_x^2},\ 0 \le \mathrm{d}_x \le R_{\mathrm{r}}. \tag{3.13}$$

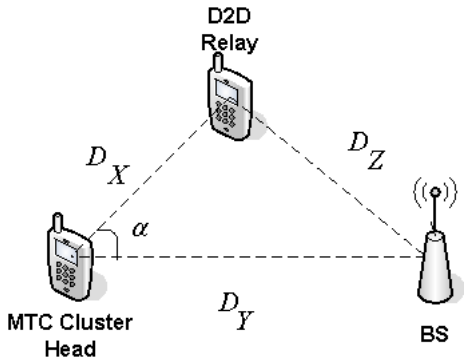

Figure 3.6: The topology of a D2D-assisted MTC link.

Furthermore, we assume that ϕ, the angle between the D2D relay, MTCCH, and the BS, is uniformly distributed between $[-\pi/2, \pi/2]$, ($f_\Phi(\phi) = 1/\pi$). By the law of cosines, we have: $D_Z = \sqrt{D_X^2 + D_Y^2 - 2D_X D_Y \cos\phi}$. The following lemma provides an expression for the distribution function of D_Z.

Lemma 3.

$$f_{D_Z}(d_z) = \frac{2d_z}{\pi\mu_m^2},\ 0 \le d_z \le \sqrt{\pi}\mu_m \tag{3.14}$$

Proof : *See Appendix 8.2.*

Let us denote the channel SINR between nodes i and j by $\gamma_{i,j}$. We define the number of all D2D relay users located in the assist region of an MTCCH located at x_i as $N_{\mathrm{r}} = |x_j \in \Phi_{\mathrm{D}}, x_j \neq x_i| \cap \mathscr{A}_r(x_i, R_{\mathrm{r}})$. N_{r} is a Poisson random variable with mean $\pi R_{\mathrm{r}}^2 \lambda_{\mathrm{D}}$. It should be noted that N_{r} is not a function of relay users' locations x_j. Thus, the probability that the MTCCH i cannot find any potential D2D relay within the assist region can be obtained as [205]: $\mathscr{P}(N_{\mathrm{r}} = 0) = e^{-\pi R_{\mathrm{r}}^2 \lambda_{\mathrm{D}}}$. Consequently, the probability that the MTCCH i can find at least one potential D2D relay is expressed as $\mathscr{P}(N_{\mathrm{r}} \geq 1) = 1 - \mathscr{P}(N_{\mathrm{r}} = 0) = 1 - e^{-\pi R_{\mathrm{r}}^2 \lambda_{\mathrm{D}}}$. In this paper, we assume that one D2D relay is able to support multiple MTCCHs, provided that it is within the assisting region of multiple MTCCHs. Although it is possible that one MTCCH can use multiple relays, for simplicity, we assume that each MTCCH can only have one D2D relay. This assumption reduces the overheads associated with relay association.

The aggregate interference at a typical D2D user is the interference from cellular transmitters and other D2D transmitters:

$$I_{\mathrm{tot,D}} = \sum_{k \in \Phi_{\mathrm{C}}} P_C h_{k0} l(k,0) + \sum_{k \in \tilde{\Phi}_{\mathrm{D}} \setminus 0} \hat{P}_{\mathrm{D}} h_{k0} l(k,0), \tag{3.15}$$

where $\tilde{\Phi}_{\mathrm{D}}$ is a PPP representing the set of effective D2D transmitters with intensity $\tilde{\lambda}_{\mathrm{D}} = \kappa \rho \lambda_{\mathrm{D}}$; and ρ is the transmission probability of a D2D user derived in Section 3.3.2.

Lemma 4. *The Laplace transform of $I_{tot,D}$ can be characterized as*

$$\mathscr{L}_{I_{tot,D}}(s) = \exp\left(\frac{-\lambda_C \pi P_C^{2/\alpha} - \tilde{\lambda}_D \pi \hat{P}_D^{2/\alpha}}{\mathrm{sinc}(\frac{2}{\alpha})} s^{2/\alpha} \right). \tag{3.16}$$

Theorem 2. *In interference-limited network ($\sigma^2 = 0$) and for a generic path-loss exponent α, the probability that a typical UE i is in D2D mode can be expressed as*

$$q = \mathscr{P}(\gamma_{i,0} \geq \theta_D) = \frac{1 - e^{-\mu_d^2 (a_2 + a_3)}}{(a_2 + a_3)\, \mu_d^2} \tag{3.17}$$

where $a_2 = \left(\left(\pi \lambda_C \theta_D^{\frac{2}{\alpha}} \right) / \left(\mathrm{sinc}(\frac{2}{\alpha}) \right) \right) P_C^{\frac{2}{\alpha}} \hat{P}_D^{-\frac{2}{\alpha}}$*;* $a_3 = (\pi \tilde{\lambda}_D \theta_D^{\frac{2}{\alpha}}) / (\mathrm{sinc}(\frac{2}{\alpha}))$*; and* μ_d *is the maximum allowable distance between a D2D pair*[3].

Proof. Since $h_0 \sim \exp(1)$, then $\mathscr{P}(h_0 \geq x) = e^{-x}$, then we can write the following:

$$\begin{aligned}
\mathscr{P}(\gamma_{i,0} \geq \theta_{\mathrm{D}}) &= \mathscr{P}\left(h_0 \geq \theta_{\mathrm{D}} l(s,0)^{-1} \hat{P}_{\mathrm{D}}^{-1} (I_{\mathrm{tot,D}} + \sigma^2)\right) \\
&= \mathrm{E}\left[\exp\left(-\theta_{\mathrm{D}} l(s,0)^{-1} \hat{P}_{\mathrm{D}}^{-1} (I_{\mathrm{tot,D}} + \sigma^2)\right)\right] \\
&\overset{(a)}{=} \mathrm{E}_X\left[\exp\left(-a_1 X - a_2 X^{2/\alpha} - a_3 X^{2/\alpha}\right)\right] \\
&\overset{(b)}{=} \int_0^{\mu_{\mathrm{d}}} \exp\left(-(a_2 + a_3) r^2\right) \frac{2r}{\mu_{\mathrm{d}}^2} dr \\
&= \frac{1 - e^{-\mu_{\mathrm{d}}^2 (a_2 + a_3)}}{(a_2 + a_3)\, \mu_{\mathrm{d}}^2},
\end{aligned}$$

where in (a), $X = \|i - j\|^{\alpha}$, $a_1 = \sigma^2 \theta_{\mathrm{D}} \hat{P}_{\mathrm{D}}^{-1}$; and (b) comes from the fact of ignoring the noise $\sigma^2 = 0$ and using the uniform distribution PDF between a D2D pair with maximum allowable distance of μ_{d} (similar to Eq.(3.12)). □

Note that from Eq. (3.17), as $\mu_{\mathrm{d}} \to 0$, $q \to 1$; and as $\mu_{\mathrm{d}} \to \infty$, $q \to 0$. If a typical UE i cannot be in D2D mode, then it becomes a cellular user, such that $\mathscr{P}(\delta_i = \delta_{\mathrm{C}}) = 1 - q = 1 - \mathscr{P}(\delta_i = \delta_{\mathrm{D}})$.

3.3.2 Transmission Probability of a D2D User

Similar to Section 3.2.4, we obtain the expected RF energy harvesting rate for a D2D user; however this time we do not limit the harvesting region to a specific region, but rather we extend it to the whole space. That is said, we obtain the expected RF energy harvesting rate as in the following theorem.

Theorem 3. *The expected RF energy harvesting rate, when the path loss exponent* $\alpha = 4$*, is ex-*

[3]Throughout the paper, we use the notation f^{-1} to denote the inverse of f.

pressed as

$$\eta = \frac{\pi^{3/2} \upsilon_e \sqrt{P_C} \tilde{\lambda}_C \lambda_D}{4} \int_0^\infty Q\left(\frac{-Nx}{\sqrt{x+\sigma_n^2}}\right) x^{-3/2} e^{-\frac{\pi^4 \tilde{\lambda}_C^2 P_C}{16x}} dx. \tag{3.18}$$

The energy utilization rate υ is defined as the number of units of energy required per second by a D2D user [226].

Theorem 4. *The energy utilization rate can be expressed as*

$$\upsilon = \kappa \lambda_D \exp\left(-\lambda_D \pi \left(\frac{\hat{P}_D}{\varepsilon}\right)^{2/\alpha} \Gamma\left(1+\frac{2}{\alpha}\right)\right). \tag{3.19}$$

Proof. Without loss of generality, the transmission region $R_0(\varepsilon) \subset \mathbf{R}^2$ around a typical D2D user is random and defined as the range within which other nodes can receive its signal with a power above a decoding threshold ε. This allows a receiver to satisfy a minimum SINR so that the two nodes are connected [227]. We define the transmission region as [213]:

$$\begin{aligned} R_0(\varepsilon) &= \left\{x \in \mathbf{R}^2 : \hat{P}_{\mathrm{D}} l(x,0) h_{x0} > \varepsilon\right\} \\ &= \left\{x \in \mathbf{R}^2 : \|x\| < \mu_{\mathrm{d}}, \mu_{\mathrm{d}} = \left(\frac{\hat{P}_{\mathrm{D}} h_{x0}}{\varepsilon}\right)^{1/\alpha}\right\}, \end{aligned} \tag{3.20}$$

where ε is the minimum power level required to be successfully heard (may or may not decode successfully). The area of the transmission region is defined as [226]:

$$|R_0(\varepsilon)| = \int_{\mathbf{R}^2} \Pi_{y \in \Phi_{\mathrm{D}}} \mathbb{1}(\hat{P}_{\mathrm{D}} l(y,0) h_{y0} > \varepsilon) dx, \tag{3.21}$$

where the indicator function $\mathbb{1}(A)$ for event A is equal to one if A occurs or else is zero. The average

transmission area is:

$$\begin{aligned}
\mathrm{E}[|R_y(\varepsilon)|] &= \mathrm{E}\mathrm{E}^0_{\Phi_\mathrm{D}}[|R_0(\varepsilon)|] = \mathrm{E}\mathrm{E}_{\Phi_\mathrm{D}}[|R_0(\varepsilon)|] \\
&= \mathrm{E}_h \int_{\mathbf{R}^2} \mathbf{E}_{\Phi_\mathrm{D}} \Pi_{y\in\Phi_\mathrm{D}} \mathbb{1}(\hat{P}_\mathrm{D}\|x\|^{-\alpha} h_0 > \varepsilon) dx \\
&= \mathrm{E}_h \int_{\mathbf{R}^2} e^{-\lambda_\mathrm{D}\mathbb{1}(\hat{P}_\mathrm{D}\|x\|^{-\alpha}h_0)>\varepsilon} dx \\
&= \mathrm{E}_h \int_{\mathbf{R}^2} e^{-\lambda_\mathrm{D}\mathbb{1}(\|x\|<\mu_\mathrm{d})} dx \\
&= \mathrm{E}_h \left(e^{-\lambda_\mathrm{D}\pi\mu_\mathrm{d}^2}\right) = e^{-\lambda_\mathrm{D}\pi\mathbf{E}_h[\mu_\mathrm{d}^2]} \\
&\overset{(a)}{=} \exp\left(-\lambda_\mathrm{D}\pi\left(\frac{\hat{P}_\mathrm{D}}{\varepsilon}\right)^{2/\alpha}\Gamma\left(1+\frac{2}{\alpha}\right)\right),
\end{aligned} \tag{3.22}$$

where (a) comes from the fact that: $\mathrm{E}_h[\mu_\mathrm{d}^2] = \mathrm{E}_h\left[(\frac{\hat{P}_\mathrm{D}h_0}{\varepsilon})^{\frac{2}{\alpha}}\right] = (\frac{\hat{P}_\mathrm{D}}{\varepsilon})^{\frac{2}{\alpha}}\mathrm{E}_h(h_0^{\frac{2}{\alpha}})$, and $\mathrm{E}_h[h_x^m] = \Gamma(1+m)$. The energy utilization rate is expressed as: $\upsilon = \kappa\lambda_\mathrm{D}\mathrm{E}[|R_y(\varepsilon)|]$. Substituting in Eq. (3.22) completes the proof. □

Let $S_{t,k}$ denote the battery level at time t for D2D user k. The dynamics of the battery level can be captured as: $S_{t,k} = \min\left\{S_{t-1,k} + \eta - \upsilon\mathbb{1}\left(S_{t-1,k} \geq \upsilon\right), G\right\}$, where G is the battery capacity, which we assume is identical for all users. We define the transmission probability ρ of a D2D user as [228]:

$$\rho = \lim_{n\to\infty} \frac{1}{n}\sum_{t=1}^{n} \mathrm{E}\left[\mathbb{1}\left(S_{t,k} \geq \upsilon\right)\right]. \tag{3.23}$$

Assuming infinite battery capacity[4] and a saturated buffer model (i.e., D2D users always have traffic to send), and using calculations in [228], we can express the transmission probability of D2D user as

$$\rho = \min\left(1, \frac{\eta}{\upsilon}\right) \tag{3.24}$$

[4]The limit of exceeding the battery capacity is negligible when the capacity is much larger than the average stored energy. Thus, the infinite battery capacity assumption can be regarded as an approximation.

3.3.3 Spectral Efficiency Analysis

In this section, we characterize the spectral efficiency of cellular, D2D and MTC links in both direct and relay modes by calculating $\mathrm{E}[\log(1+\mathrm{SINR})]$ in each of these cases. For the D2D-assisted MTC mode, instead of assuming that the transmissions in the first and second time slots are independent, we introduce the temporal and spatial correlation in order to make the analysis more realistic and practical.

3.3.3.1 Cellular Spectral Efficiency Analysis

Similar to [1], we adopt the spatial Aloha access scheme for MTC devices, where the device transmits with probability ϖ in each time slot and refrains from transmission with probability $1-\varpi$. Thus, the effective cochannel MTC interferers form a thinning HPPP $\tilde{\Phi}_{\mathrm{M}}$ from Φ_{M} with intensity $\tilde{\lambda}_{\mathrm{M}} = \varpi\lambda_{\mathrm{M}}$. Without loss of generality, the aggregate interference at a typical BS comes from cellular transmitters in other cells; D2D transmitters and MTC devices in all cells. It is expressed as

$$I_{\mathrm{BS}} = \sum_{k\in\Phi_{\mathrm{C}}\cap\mathscr{A}^c} P_{\mathrm{C}} h_{k0} l(k,0) + \sum_{k\in\tilde{\Phi}_{\mathrm{D}}} \hat{P}_{\mathrm{D}} h_{k0} l(k,0) + \sum_{k\in\tilde{\Phi}_{\mathrm{M}}} P_{\mathrm{M}} h_{k0} l(k,0). \tag{3.25}$$

Lemma 5. *The Laplace transform of I_{BS} is characterized as*

$$\begin{aligned}\mathscr{L}_{I_{BS}}(s) = &\exp\left(\frac{-\tilde{\lambda}_D \hat{P}_D^{2/\alpha} - \tilde{\lambda}_M P_M^{2/\alpha}}{\mathrm{sinc}(\frac{2}{\alpha})}\pi s^{2/\alpha}\right) \\ &\cdot \exp\left(\frac{-2\pi\lambda_B P_C s}{(\alpha-2)R_B^{\alpha-2}} {}_2F_1\left(1, 1-\frac{2}{\alpha}; 2-\frac{2}{\alpha}; -\frac{sP_C}{R_B^{\alpha}}\right)\right).\end{aligned} \tag{3.26}$$

Proof : *Similar calculations to Appendix 8.1.*

From (3.26), increasing P_{C}, P_{M} or $\hat{P}_{\mathrm{D}}$ increases the amount of interference at the BS, with P_{C} having the greatest impact due to the larger transmit power when compared to D2D or MTC devices. Furthermore, increasing $\tilde{\lambda}_{\mathrm{D}}$ or $\tilde{\lambda}_{\mathrm{M}}$ can negatively impact the cellular spectral efficiency.

That is why it is important to carefully design κ to protect cellular transmissions, without negatively impacting D2D and MTC spectral efficiency.

Theorem 5. *In an interference-limited network ($\sigma^2 = 0$) and for $\alpha = 4$, we have*

$$\mathscr{P}\left(\gamma_0 \geq \theta_C\right) = \frac{2}{R_B^2} \int_0^{R_B} \exp\left(-b_2 r^2 - b_3 r^2 \tan^{-1}\left(b_3 r^2\right)\right) r dr,$$

where $b_2 = (1/2)\pi^2 \left(\tilde{\lambda}_D \hat{P}_D^{1/2} + \tilde{\lambda}_M P_M^{1/2}\right) P_C^{-1/2} \theta_C^{1/2}$*; and* $b_3 = R_B^{-2} \theta_C^{1/2}$.

Proof. We use similar calculation steps as in Theorem 2, with the assumption of CUs being uniformly distributed within a fixed region [229]. □

From Theorem 5, it can be seen that increasing D2D and MTC intensities decreases the cellular coverage probability.

Theorem 6. *The spatially averaged spectral efficiency of the cellular transmitters, R_C, can be characterized as*

$$\begin{aligned} R_C = \frac{343\sqrt{7}\lambda_B^{7/2}}{20\sqrt{2}\lambda_C} \left[\left(\frac{7\lambda_B}{2}\right)^{-5/2} - \left(\frac{7\lambda_B}{2} + \lambda_C\right)^{-5/2}\right] \cdot \\ \int_{r>0} 2\pi r \lambda_B e^{-\pi\lambda_B r^2} \int_{t>0} e^{-\sigma_n^2 r^\alpha \left(2^t - 1\right)} \mathscr{L}_{I_{BS}}\left(r^\alpha \left(2^t - 1\right)\right) dt dr, \end{aligned} \tag{3.27}$$

Proof : *See Appendix 8.3.*

Remarks: From (3.27), we note that the intensity of cellular transmitters, λ_{C}, is only included in the denominator of the non-integral term of R_{C}. Thus, as λ_{C} increases, R_{C} decreases.

3.3.3.2 D2D Spectral Efficiency Analysis

Theorem 7. *Using similar calculation steps as in Appendix 8.3, we can express the spatially averaged spectral efficiency of the D2D links, R_D, as*

$$R_D^d = \int_0^{\mu_d} \frac{2\kappa\rho d_y}{\mu_d^2} \int_0^{\infty} e^{-\sigma_n^2 d_y^\alpha \left(2^t - 1\right)} \mathscr{L}_{I_{tot,D}}\left(d_y^\alpha \left(2^t - 1\right)\right) dt d d_y.$$

3.3.3.3 MTC Spectral Efficiency Analysis

Direct MTC Link

The following theorem provides an expression for the average SIR probability at a typical BS for the direct MTC link.

Theorem 8. *In interference-limited network ($\sigma^2 = 0$) and for path-loss exponent $\alpha = 4$, we have*

$$\mathscr{P}\left(\gamma_{i,0} \geq \theta_M\right) = \frac{2r}{\mu_m^2} \int_0^{\mu_m} \exp\left(-c_2 r^2 - c_3 r^2 \tan^{-1}\left(c_3 r^2\right)\right) r dr, \tag{3.28}$$

where $c_2 = (1/2)\pi^2 \left(\tilde{\lambda}_D \hat{P}_D^{1/2} + \tilde{\lambda}_M P_M^{1/2}\right) P_M^{-1/2} \theta_M^{1/2}$*; and* $c_3 = R_B^{-2} \theta_M^{1/2} P_M^{-1/2} P_C^{1/2}$.

Proof: Similar derivation steps as in Theorem 2.

Theorem 9. *The spatially averaged spectral efficiency of the direct MTC links, R_M^d, can be characterized as*

$$R_M^d = \int_0^{\mu_m} \frac{2\varpi d_y}{\mu_m^2} \int_{t>0} e^{-\sigma_n^2 d_y^{\alpha}\left(2^t - 1\right)} \mathscr{L}_{I_{BS}}\left(d_y^{\alpha}\left(2^t - 1\right)\right) dt d d_y, \tag{3.29}$$

D2D-assisted MTC Link

Cooperation introduces a correlation in the aggregate interference due to receivers being closely located to each other, thereby affecting the system performance and rendering the analysis much more complex [230]. In this section, we derive the average SIR of the MTC relay link under correlated interference, where the interference at the relay and at the BS originate from the same set of interferers [231] (see Fig. 3.5).

We shall ignore the noise ($\sigma^2 = 0$) and proceed with the calculations for interference-limited networks. Let us first consider the case when there is a single D2D relay available in the assist region. Later, we will extend the result to when multiple D2D relays exist within the transmitter's assist region.

We consider that both source node s and relay node r work in time division duplex (TDD) mode, i.e., only one node transmits at any time in the two-hop relay link. The aggregated interference at the relay node r during time slot t:

$$I_r^t = \sum_{j \in \Phi_{\mathrm{C}}^t \cap \mathscr{A}} P_{\mathrm{C}} h_{jr} l(j,r) + \sum_{j \in \Phi_{\mathrm{C}}^t \cap \mathscr{A}^c} P_{\mathrm{C}} h_{jr} l(j,r) + \sum_{j \in \tilde{\Phi}_{\mathrm{D}}^t \setminus \{s\}} \hat{P}_{\mathrm{D}} h_{jr} l(j,r).$$

Similarly, the aggregated interference at destination node d is:

$$I_d^t = \sum_{j \in \Phi_{\mathrm{C}}^t \cap \mathscr{A}^c} P_{\mathrm{C}} h_{jd} l(j,d) + \sum_{j \in \tilde{\Phi}_{\mathrm{D}}^t \setminus \{s\}} \hat{P}_{\mathrm{D}} h_{jd} l(j,d) + \sum_{j \in \tilde{\Phi}_{\mathrm{M}}^t \setminus \{s\}} P_{\mathrm{M}} h_{jd} l(j,d).$$

Then, the channel SIR between the source and relay is given by $\gamma_{s,r} = P_{\mathrm{M}} h_{sr} l(s,r)/I_r^t$, while the channel SIR between the relay and destination is given by $\gamma_{r,d} = \hat{P}_{\mathrm{D}} h_{rd} l(r,d)/I_d^t$. The following theorem provides an expression for the average SIR probability $\mathscr{P}\left(\gamma_{s,r} \geq \theta_{\mathrm{M}} \cap \gamma_{r,d} \geq \theta_{\mathrm{M}}\right)$.

Theorem 10. *In interference-limited network ($\sigma^2 = 0$) and for generic path-loss exponent α, we have*

$$\begin{aligned} \mathscr{P}\left(\gamma_{s,r} \geq \theta_M \cap \gamma_{r,d} \geq \theta_M\right) &\approx \exp\left(-\lambda_C \int_{R_B}^{\infty} 1 - \frac{1}{B_1(x)B_2(x)} dx\right) \\ &\cdot \exp\left(-\lambda_C \int_0^{R_B} 1 - \frac{1}{B_2(x)} dx\right) \exp\left(-\tilde{\lambda}_M \int_0^{\infty} 1 - \frac{1}{B_1(x)} dx\right) \\ &\cdot \exp\left(-\tilde{\lambda}_D \int_0^{\infty} 1 - \frac{1}{B_1(x)B_2(x)} dx\right), \end{aligned} \tag{3.30}$$

where $B_1(x) \approx 1 + \left(\theta_M l(x,d) \hat{P}_D^{-1}\right)^{2/\alpha} 4\pi\mu^2/9$; $B_2(x) \approx 1 + \left(\theta_M l(x,r) P_M^{-1}\right)^{2/\alpha} \mathrm{E}[\|s-r\|]^2$; *and* $\mathrm{E}[\|s-r\|]$ *is given in Eq. (8.6).*

Proof : *See Appendix 8.4.*

Extending the above to when multiple D2D relays exist in the assist region of the MTC CH, we obtain the same as Eq. (3.30), but with $B_2(x) \approx \prod_{n=1}^{N_{\mathrm{r}}} \left(1 + \left(\theta_{\mathrm{M}} l(x,n) P_{\mathrm{M}}^{-1}\right)^{2/\alpha} \mathrm{E}[\|s-r\|]^2\right)$.

Theorem 11. *The spatially averaged spectral efficiency of the D2D-assisted MTC links, R_M^r, can*

be characterized as

$$R_M^r \approx \varpi \int_0^{\infty} \Bigg[\exp\left(-\lambda_C \int_{R_B}^{\infty} 1 - \frac{1}{T_1(x,t)T_2(x,t)} dx \right) \exp\left(-\tilde{\lambda}_D \int_0^{\infty} 1 - \frac{1}{T_1(x,t)T_2(x,t)} dx \right)$$

$$\exp\left(-\lambda_C \int_0^{R_B} 1 - \frac{1}{T_2(x,t)} dx \right) \exp\left(-\tilde{\lambda}_M \int_0^{\infty} 1 - \frac{1}{T_1(x,t)} dx \right) \Bigg] dt,$$

where $T_1(x,t) = 1 + \left((2^t - 1) l(x,d) \hat{P}_D^{-1}\right)^{2/\alpha} 4\pi\mu^2/9$;
$T_2(x,t) = \prod_{n=1}^{N_r} \left(1 + \left((2^t - 1) l(x,n) P_M^{-1}\right)^{2/\alpha} \mathrm{E}[\|s - r\|]^2\right)$.

Remarks: Increasing any of the intensities of cellular, D2D or MTC devices decreases R_M^r.

We will be using the obtained expressions in Section 3.3.4 to study the impact of different parameters, such as the cellular intensity, number of channels, and spectrum partition factor, on the spectral efficiency of MTC, D2D and cellular networks.

3.3.4 Results and Analysis

In this section, we present analytical and simulation results for D2D-assisted MTC communication as an underlay to the uplink cellular network, with energy harvesting D2D users. The parameters in plotting the numerical and simulation results are summarized in Table 3.2 unless otherwise specified[5]. In Fig. 3.7, we plot the average MTC spectral efficiency for both the direct MTC mode and D2D-assisted MTC mode versus the intensity of cellular users. For the direct MTC mode, a larger population of cellular users negatively impact the MTC spectral efficiency due to the larger cellular and D2D interference on MTC links. However this is not true for the D2D-assisted MTC mode, where a larger population of cellular users positively impact the MTC spectral efficiency. This is explained by the fact that the average D2D transmission probability increases with λ_C, as shown in Fig. 3.9, due to D2D users being able to harvest more RF power from ambient cellular

[5]We used similar parameters values to [209] and [232].

Table 3.2: Simulation/Numerical Parameters

Radius of the macrocell R_{B}	788 meters (inter-BS distance of 1500 meters)
Density of macrocells λ_{B}	$1/\left(\pi R_{\mathrm{B}}^2\right)$
Density of UEs λ_{U}	$10\lambda_{\mathrm{B}}$
Density of MTC devices λ_{M}	$2\lambda_{\mathrm{D}}$
Power of a cellular user P_{C}	200 mW
Power of D2D users, $\hat{P}_{\mathrm{D}}$, and MTC devices, P_{M}	2 mW
The total number of samples N	5000
Radius of relay-assisted region R_{r}	100 meters
Target SINR threshold θ_{D}, θ_{C}, θ_{M}	10 dB
Total number of available channels $\lvert B\rvert$	10
Spectrum partition factor κ	0.5
Aloha access probability ϖ for MTC devices	0.5
Path-loss exponent α	4
RF energy conversion efficiency υ_{e}	0.6 [218]

interference. This increases the number of D2D transmissions that can be supported in the network, thereby offloading more MTC traffic on the shorter D2D links. Furthermore, it is interesting to see that with $\kappa = 0.8$, we can achieve higher spectral efficiency than a smaller κ; however beyond a specific λ_{C}, improvement in spectral efficiency can no longer be seen, since the D2D users are less capable of harvesting RF power from the $(1-\kappa)|B|$ subchannels, as they have now access to a larger cellular spectrum proportion.

To elaborate further on this, we capture the impact that κ has on the coverage probability of MTC devices in Fig 3.8. The figure shows that as κ increases, i.e., a larger fraction of the spectrum is available for D2D transmissions, the coverage probability of MTC devices increases due to offloading more MTC traffic on the shorter D2D links.

Fig. 3.9 depicts the D2D transmission probability versus λ_{C} for different values of $|B|$. When more channels are available in the network, D2D users can harvest more RF power from them. As can be seen from Fig. 3.9, a higher number of channels does not necessarily provide larger benefits to D2D users, as $|B| = 30$ channels still give comparable performance to $|B| = 60$ channels, especially when λ_{C} is small. On the other hand, as $|B|$ becomes smaller, the transmission probability of D2D users starts decreasing due to reducing the number of subchannels D2D users can harvest from.

Fig. 3.10 shows the impact of ρ on the cellular spectral efficiency R_{C}. As the transmission probability, ρ, of D2D users increases, R_{C} decreases, since more active D2D users means more interference at cellular transmitters. As the spectrum partition factor, κ, increases, more D2D users are accessing the spectrum thereby creating more interference in the cellular network. However, note that it is difficult to achieve $\rho = 1$ as κ increases, since D2D users will harvest less RF power from $(1-\kappa)|B|$ subchannels. Thus, this figure is just to show the impact that ρ can have on R_{C}.

To show the balance between efficiency and fairness among D2D and cellular transmitters that are sharing the cellular spectrum, we plot the weighted proportional-fair spectral efficiency, R_p in Fig. 3.11. It can be expressed as [1]: $R_p = w_{\mathrm{C}} \log R_{\mathrm{C}} + (1-w_{\mathrm{C}}) \log R_{\mathrm{D}}$, where $0 \leq w_C \leq 1$. Fig. 3.11 shows that as the probability of UEs operating in D2D mode, q, increases from 0.5 to 0.7, so does the proportional-fair spectral efficiency R_p of the whole network. However, when $q = 0.9$, i.e., there is aggressive D2D offloading, R_p decreases as explained in [233]. Furthermore, as the spectrum partition factor κ increases, R_p first increases and then decreases, which reveals an interesting trade-off between cellular users, D2D users and the optimal κ that maximizes R_p. For instance, for $q = 0.7$, R_p is maximized when $\kappa = 0.2$; and as q decreases to 0.5, the maximum R_p is achieved when $\kappa = 0.3$. After that, as κ increases further, R_p starts decreasing mainly due to two reasons: 1) increasing the interference at cellular transmitters from D2D links, which negatively affects the cellular spectral efficiency; and 2) increasing κ means the intensity of cellular users not using $\kappa|B|$ subchannels, $\tilde{\Phi}_{\mathrm{C}}$, decreases, which reduces the probability of D2D users harvesting enough RF energy from ambient cellular signals, thereby decreasing their transmission probability. This shows that RF energy harvesting can be beneficial to the whole network when κ is small. Using the results of Fig. 3.7 and Fig. 3.11, we conclude that choosing a smaller value for κ (for instance $\kappa = 0.2$), with more UEs operating in D2D mode, we can target mainly two important performance criteria: 1) a balance and fairness among cellular and D2D users; and 2) a high MTC spectral efficiency from offloading the traffic onto D2D links, especially in dense cellular environment.

Finally, Fig. 3.12 shows the average D2D spectral efficiency, R_{D}, in terms of λ_C for different

values of $|B|$. For $|B| > 10$, as λ_C increases, R_{D} increases due to an increase in the D2D transmission probability ρ (see Fig. 3.9), without being negatively impacted by an increase in cellular interference at D2D users. However, this is not true when the number of channels is small and D2D users cannot harvest enough energy nor increase their spectrum access. Also note that for $|B| = 10$, R_{D} becomes stable beyond $\lambda_C \approx 7\lambda_B$ and does not improve anymore, unlike the case of $|B| = 40$, mainly due to limiting the amount of harvested RF power.

3.3.5 Conclusions

In this work, we have analyzed the spectral efficiency and coverage probability of D2D-assisted MTC communications under spatially correlated interference using stochastic geometry. First, we analytically characterized the D2D transmission probability in terms of RF energy harvesting and energy utilization rates. Second, we derived expressions for the spectral efficiency in order to study the impact of RF energy harvesting on system performance. Simulation results have shown that a small spectrum partition factor κ ($\kappa = 0.2$ or $\kappa = 0.3$ when 70% or 50% of UEs operate in D2D mode, respectively), combined with an adequate number of available channels in the network ($|B| = 30$ to 40) can achieve i) a balance and fairness in weighted spectral efficiency among D2D and cellular users that are sharing the spectrum; ii) a higher D2D transmission probability; and iii) a relatively high MTC and D2D spectral efficiency in a dense cellular environment.

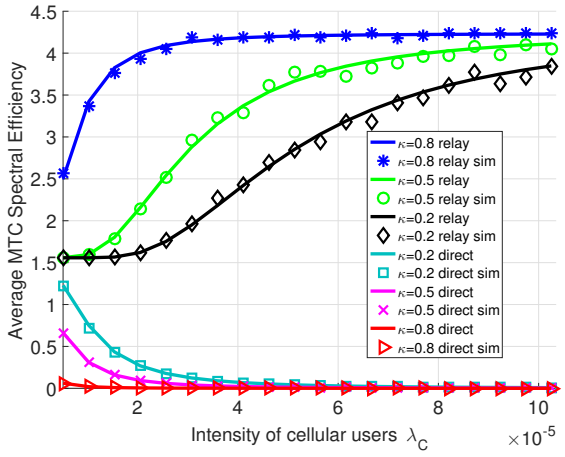

Figure 3.7: The average MTC spectral efficiency in terms of λ_C for different values of κ ($\lambda_D = 10\lambda_B$).

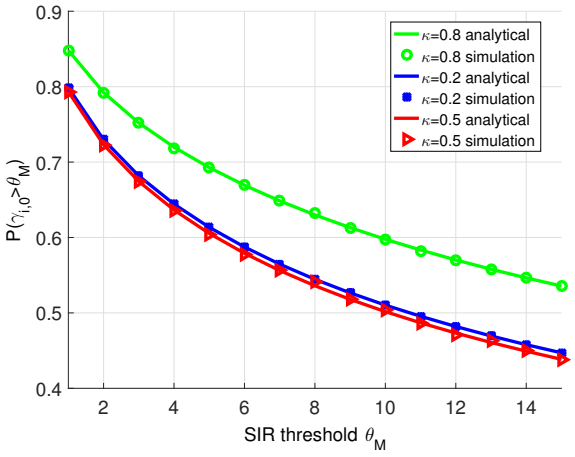

Figure 3.8: MTC coverage probability in terms of θ_M for different κ.

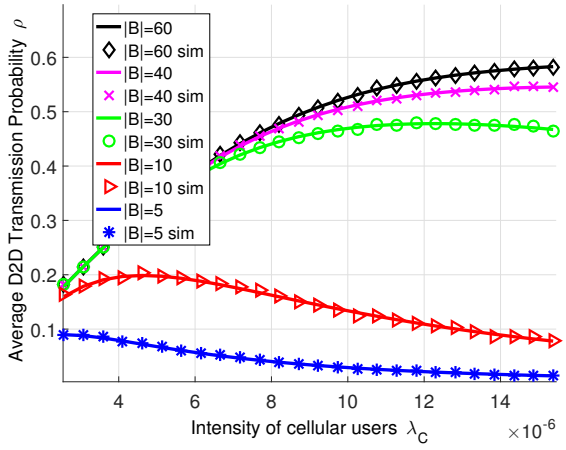

Figure 3.9: The average D2D transmission probability ρ in terms of λ_C for different values of $|B|$ ($\kappa = 0.1$).

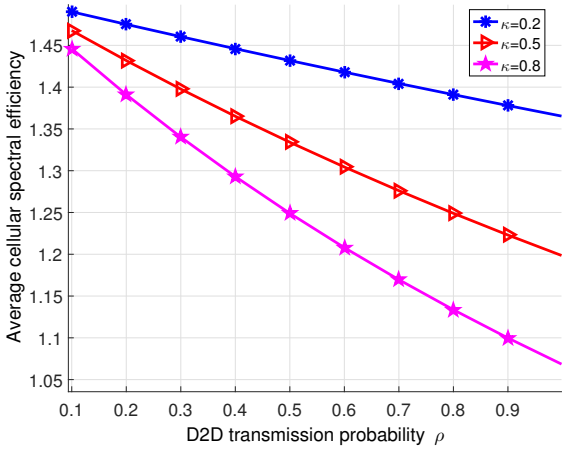

Figure 3.10: The average cellular spectral efficiency, R_C, in terms of transmission probability, ρ, for different values of κ.

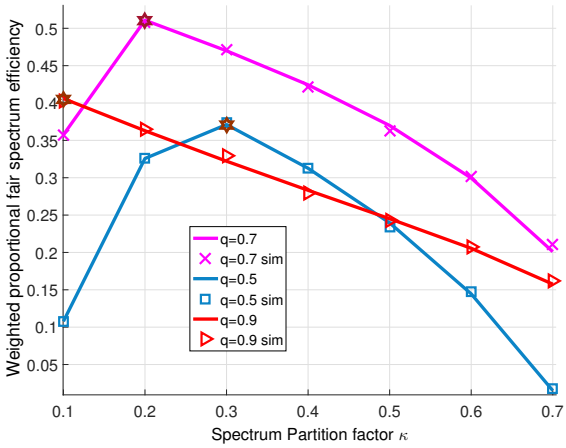

Figure 3.11: The weighted proportional-fairness spectral efficiency versus κ for different values of q ($\lambda_D = 10\lambda_B$; $w_C = 0.65$).

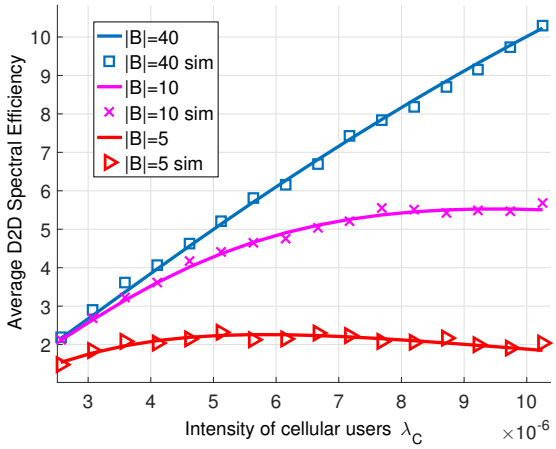

Figure 3.12: The average D2D spectral efficiency in terms of λ_C for different values of $|B|$.

Chapter 4

D2D Spatial Spectrum Sensing and Cyber-Security for Enabling CPS over Cellular Networks

Security of CPS is also an interesting aspect that we specifically study in this chapter and in Chapter 6. The security threats of CPS are made easier first with the large volume of data that is constantly flowing through the network, and second with the lack of qualified security experts. All this makes the monitoring of sensitive information a challenging task for analysts. Different approaches can be taken in this regard such as implementing advanced security controls (authentication), monitoring of real-time data streams, implementing advanced anomaly detection techniques by using neuromorphic computing for instance, real-time surveillance through computer vision and visualization techniques, and so on [234].

In this chapter, through a case study we discuss about how spatial spectrum sensing in D2D communications can help support the massive number of devices attempting to access the licensed cellular spectrum. We then present a low-complexity lightweight approach to secure the in-proximity CPS communications. Finally, we present some results to study the impact of spatial sensing region on the secure successful transmissions.

4.1 System Model

In the realm of cyber-physical systems, there is a large amount of data that is being sensed, collected and transmitted, which place security threats under the spotlight of attention. This is especially true for the more vulnerable direct connections between proximity devices, which in turn degrade system's performance. There are different reasons why in-proximity D2D connections are more vulnerable to security flaws: D2D devices have i) limited computational capabilities to employ data confidentiality, privacy preservation and authentication; ii) the semi- or fully-autonomous security management (mutual authentication, key arrangement, etc.) [235]; and iii) the high computational overhead cost of cryptographic solutions [236]. There have been some development of low-complex and lightweight ciphers such as PRESENT [237]; however such solutions can be time consuming and costly in terms of high power consumption as well as the complexity of key management [238, 239]; that is why research efforts should be pushed toward simpler solutions than cryptography.

To mitigate the potential D2D security threats such as eavesdropping, data fabrication and privacy violation threats, we turn towards a lightweight low-complexity approach by exploiting the physical characteristics of the wireless channels, by defining a D2D spatial transmission region that can guarantee a minimum secrecy rate. By doing so, we are able to derive the detection probability that D2D link is secure.

Mode Selection: A potential D2D user is a user with D2D traffic which can either use the cellular or the D2D mode for communications based on one or a combination of different selection criteria. This means that a potential D2D user can switch between D2D and conventional cellular communications. For this case study, we use distance-based selection threshold μ [240]. Let L_{C} and L_{D} be random variables representing the link lengths of a typical CU and D2D user, respectively. More specific, a user is in D2D mode if the transceiver distance L_{D} is smaller than μ. We assume that the D2D receiver is uniformly distributed within a circle centered at user i located at

location x_i with a radius of D, as $\mathscr{B}(x_i, D)$ [240], with probability density function (PDF):

$$f_{\mathrm{D}}(r) = \frac{2r}{D^2},\ 0 \leq r \leq D. \tag{4.1}$$

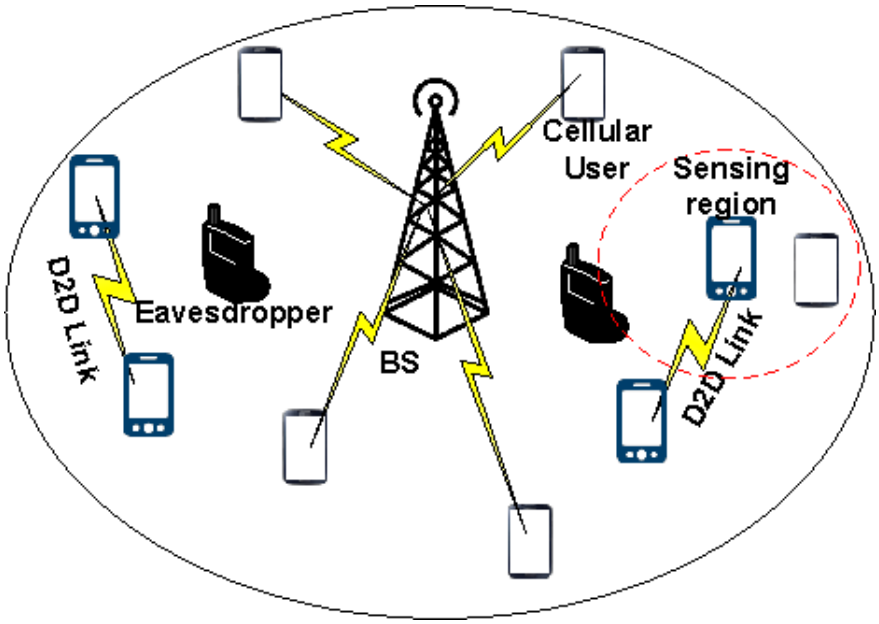

Figure 4.1: An example of a hybrid network with D2D and cellular links with eavesdroppers overhearing the D2D communication.

Fig. 4.1 illustrates a hybrid network of D2D links, cellular links and a set of eavesdroppers that attempt to overhear the D2D transmissions. Furthermore, the figure shows a spatial sensing region around D2D users. We consider an uplink cellular network, where D2D users and CUs share the licensed spectrum. The use of stochastic geometry allows us to provide an accurate model of interferers' spatial locations by averaging over all their potential topological realizations [241]. The locations of the macro BSs are modeled by a homogeneous Poisson point process (HPPP), Φ_{B} of intensity λ_{B}. Let $\mathscr{A}(k, R_{\mathrm{B}})$ denotes the coverage region of a macrocell, approximated by a disk with radius $R_{\mathrm{B}} = (\pi\lambda_{\mathrm{B}})^{-1/2}$ centered at a generic BS k. UEs are uniformly distributed in the coverage region of the corresponding BS and form an HPPP, Φ_{U} of intensity λ_{U}. The eavesdroppers form an HPPP Φ_{E} of intensity λ_{E}.

We denote by $\|i-j\|$ as the distance between any two nodes i and j. We use a power-law path-

los model where the power of the signal transmitted by UEs decays at a rate of $l(i,j) = \|i-j\|^{-\alpha}$, and $\alpha > 2$ is the path-loss exponent of both cellular and D2D transmitters. To model the small-scale fading over each channel, we use Rayleigh fading with mean one, with h_{ij} denoting the channel coefficient between nodes i and j.

For reliable communication, we assume that all users use a truncated channel inversion power control [242, 243], which ensures the average received signal power at the intended receiver (i.e., D2D receivers and BSs) is at least equal to its sensitivity. Thus, UEs will use power control $P_i = \rho L_i^{\alpha}$, for $i = \{\mathrm{C},\mathrm{D}\}$; and $\rho \ll 1$ is a constant that scales down the actual transmit power [240].

We differentiate between two different types of nodes τ_i with $i = \{\mathrm{D},\mathrm{C}\}$, for D2D user and cellular user, respectively. Let $q \in [0,1]$ be the probability that a user is a potential D2D user [240].

- **D2D user:** The UEs in D2D mode form a thinning PPP Φ_{D} from Φ_{U}, with intensity $\lambda_{\mathrm{D}} = q\lambda_{\mathrm{U}}\mathscr{P}(L_{\mathrm{D}} < \mu)$.

- **Cellular user:** The UEs in cellular mode include both cellular users and potential D2D users operating in cellular mode. Therefore, these users form a thinning PPP Φ_{C} from Φ_{U}, with intensity $\lambda_{\mathrm{C}} = (1-q)\lambda_{\mathrm{U}} + q\lambda_{\mathrm{U}}\mathscr{P}(L_{\mathrm{C}} \geq \mu)$. Note that $\Phi_{\mathrm{U}} = \Phi_{\mathrm{C}} \cup \Phi_{\mathrm{D}}$, and $\Phi_{\mathrm{D}} \cap \Phi_{\mathrm{C}} = \emptyset$.

4.2 Spatial Spectrum Sensing

A sensing region $\mathscr{A}_{\mathrm{s}}$ is defined as a circular region centered at a D2D user x_i with sensing radius R_{s}. Without loss of generality, the D2D transmitter is assumed located at the origin. A D2D transmitter opportunistically accesses the spectrum by performing energy detection on the test statistics Γ, where $\Gamma = 1/N \sum_{n=0}^{N-1} |y[n]|^2$; and $y[n]$ is defined under two different hypotheses: i) $\mathscr{H}_0$ when there are no active cellular users inside $\mathscr{A}_{\mathrm{s}}$; and ii) $\mathscr{H}_1$ when there is at least one active cellular user inside $\mathscr{A}_{\mathrm{s}}$. It is given as [244]:

$$\mathscr{H}_0 : y[n] = \sum_{i \in \phi_{\mathrm{C,a}} \cap \mathscr{A}_{\mathrm{s}}^{C}} \sqrt{P_{\mathrm{C},i} h_i \|x_i\|^{-\alpha}} s_i[n] + z[n], \tag{4.2}$$

$$\mathscr{H}_1 : y[n] = \sum_{\substack{i \in \tilde{\phi}_{\mathrm{C},a} \\ \tilde{\phi}_{\mathrm{C},a} \cap \mathscr{A}_\mathrm{s} \neq \emptyset}} \sqrt{P_{\mathrm{C},i} h_i \|x_i\|^{-\alpha}} s_i[n] + z[n], \tag{4.3}$$

where $n = 0, 1, ..., N-1$ is the sample index with N being the total number of samples; $s_i[n]$ is the nth sample of the received signal from cellular transmitter i by a typical D2D user; $z[n]$ is the Gaussian noise sample ($z[n] \sim \mathscr{N}(0, \sigma_n^2)$); and $\phi_{\mathrm{C},a}$ is a realization of $\Phi_{\mathrm{C},a}$ denoting the set of active cellular transmitters' locations; and $\mathscr{A}_\mathrm{s}^C$ is the complementary set of $\mathscr{A}_\mathrm{s}$. Let ε denotes the underlying sensing threshold. The probabilities of false alarm P_f and spatial detection P_d are given in [245] as

$$P_\mathrm{f} = \int_0^\infty \mathscr{Q}\left(\frac{\varepsilon - x - \sigma_n^2}{\sqrt{(x+\sigma_n^2)^2 / N}} \right) \sqrt{\frac{\rho}{2\pi x^3}} e^{\frac{-\rho(x-\upsilon)^2}{2\upsilon^2 x}} dx,$$
$$P_\mathrm{d} = \sum_{i=1}^{\infty} \frac{\Gamma(1+i\delta)\sin(\pi i\delta)\pi^{2i-1}(\lambda_\mathrm{B}\delta\mathbb{E}[P_c^\delta])^i}{(-1)^{i+1}(1-e^{-\lambda_\mathrm{B}\pi R_\mathrm{s}^2})i!\sin(\pi\delta)^i} \int_0^\infty \mathscr{Q}\left(\frac{\varepsilon - x - \sigma_n^2}{\sqrt{(x+\sigma_n^2)^2/N}} \right) \frac{dx}{x^{1+i\delta}} - \frac{e^{-\lambda_\mathrm{B}\pi R_\mathrm{s}^2} P_\mathrm{f}}{1 - e^{-\lambda_\mathrm{B}\pi R_\mathrm{s}^2}}, \tag{4.4}$$

where $\rho = \frac{2\mathbb{E}[P_c]^3 R_\mathrm{s}^{4-\alpha}(2\alpha-2)}{(\alpha-2)^3 R_\mathrm{B}^4 \mathbb{E}[P_c^2]}$, $\upsilon = \frac{2\mathbb{E}[P_c] R_\mathrm{s}^{2-\alpha}}{(\alpha-2)R_\mathrm{B}^2}$, $\delta = 2/\alpha$, $\mathscr{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-u^2/2} du$.

4.3 D2D Links' Secrecy Analysis

In this section, we obtain the probability of detecting that D2D link is secure by assuming that each D2D link is exposed to all the eavesdroppers. We also obtain the secure transmission region defined as the region within which eavesdroppers cannot intercept the communication with high probability.

The aggregate interference of an eavesdropper located at a distance $\|z\|$ away from the typical D2D link is the interference generated from active cellular transmitters and other active D2D

transmitters, and is given by:

$$I_{\mathrm{E}} = \sum_{k \in \Phi_{\mathrm{C},a}} P_{\mathrm{C},k} h_{k,z} l(k,z) + \sum_{k \in \Phi_{\mathrm{D},a} \setminus 0} P_{\mathrm{D},k} h_{k,z} l(k,z), \tag{4.5}$$

where $\Phi_{\mathrm{D},a}$ is approximated as an HPPP to model the locations of active D2D transmitters with intensity [245] $\lambda_{\mathrm{D},a} = \bar{\beta}\lambda_{\mathrm{D}}$; with

$$\bar{\beta} = \left(P_{\mathrm{d}} + (P_{\mathrm{f}} - P_{\mathrm{d}})\, e^{-\pi\lambda_{\mathrm{B}} R_{\mathrm{s}}^2}\right)\beta_1 + \left(1 - P_{\mathrm{d}} - (P_{\mathrm{f}} - P_{\mathrm{d}})\, e^{-\pi\lambda_{\mathrm{B}} R_{\mathrm{s}}^2}\right)\beta_0, \tag{4.6}$$

where β_1 is the spectrum access probability if the spectrum hole is correctly detected or when a false alarm occurs, while β_0 is the probability when misdetection occurs. The Laplace transform of I_E is given by [246]:

$$\mathscr{L}_{I_E}(s) = \exp\left(\frac{-\lambda_{\mathrm{C},a}\mathrm{E}\left[P_{\mathrm{C}}^{\delta}\right] - \lambda_{\mathrm{D},a}\mathrm{E}\left[P_{D}^{\delta}\right]}{\operatorname{sinc}\delta}\pi s^{\delta}\right). \tag{4.7}$$

Let $\max_{e \in \Phi_{\mathrm{E}}} \gamma_{e,0}$ denotes the eavesdropper with the most detrimental effect on D2D signal. In interference-limited networks, the average probability that a D2D link is secure is equal to the average probability that the rate of the most detrimental eavesdropper falls below a certain threshold ζ. It is expressed as [246]:

$$\begin{aligned} P_{\mathrm{s}}(\zeta) &= \mathscr{P}\left(\log\left(1 + \max_{e \in \Phi_{\mathrm{E}}} \gamma_{e,0}\right) < \zeta\right) \\ &= \exp\left(\frac{-\lambda_{\mathrm{E}} \operatorname{sinc}\delta}{\left(\lambda_{\mathrm{C},a}\mathrm{E}[P_{\mathrm{C}}^{\delta}] + \lambda_{\mathrm{D},a}\mathrm{E}[P_{\mathrm{D}}^{\delta}]\right)\mathrm{E}[P_{\mathrm{E}}^{-\delta}]\left(2^{\zeta} - 1\right)^{\delta}}\right), \end{aligned} \tag{4.8}$$

where P_{E} is the average transmit power of an eavesdropper. A D2D transmission is said to be secure if $P_{\mathrm{s}}(\zeta) \geq \upsilon_s$, where υ_s denotes the minimum required secrecy probability. Then, we can obtain

an upper bound for the secrecy rate threshold for secure communication in high SINR regime as

$$\zeta \leq \delta^{-1} \log_2 \left(\frac{-\lambda_{\mathrm{E}} \operatorname{sinc} \delta}{\left(\lambda_{\mathrm{C}} \mathrm{E}[P_{\mathrm{C}}^{\delta}] + \lambda_{\mathrm{D},a} \mathrm{E}[P_{\mathrm{D}}^{\delta}]\right) \mathrm{E}[P_{\mathrm{E}}^{-\delta}] \log \upsilon_s} \right). \tag{4.9}$$

The secure transmission region, $\mathscr{A}_{\mathrm{t}}(\mu_{\mathrm{s}}, \upsilon_{\mathrm{s}}) \subset \mathbb{R}^2$, around a typical D2D user is random and defined as the range within which eavesdroppers cannot intercept the communication with high probability. In other words, $\mathscr{A}_{\mathrm{t}}(\mu_{\mathrm{r}}, \upsilon_{\mathrm{s}})$ is the region where the set of all eavesdroppers are located outside a closed ball $\mathscr{B}\left(o, 2^{\zeta/\alpha}\|x_o\|\right)$ centered around the typical D2D user located at $\|x_o\|$ with radius $2^{\zeta/\alpha}\|x_o\|$ [247]. Therefore we can use the upper bound on ζ defined in Eq.(4.9) to define $\mathscr{A}_{\mathrm{t}}(\mu_{\mathrm{r}}, \upsilon_{\mathrm{s}})$ as:

$$\mathscr{A}_{\mathrm{t}}(\mu_{\mathrm{r}}, \upsilon_{\mathrm{s}}) = \left\{ x \in \mathbf{R}^2 : \|e - x_o\| > \mu_{\mathrm{r}} = 2^{\zeta/\alpha}\|x_o\| \right\}. \tag{4.10}$$

Then,

$$\mu_{\mathrm{r}} \leq \int_0^D 2^{\zeta/\alpha} r f_{\mathrm{D}}(r) dr = 2^{\zeta/\alpha} \frac{2D}{3}. \tag{4.11}$$

4.4 Achievable Secrecy Transmission Capacity

In the case when the packets are not successfully decoded, we assume no re-transmissions. Let θ_{D} be the signal-to-interference-plus-noise ratio (SINR) threshold for successful transmission. We can then define the mathematical expectation of the achievable secrecy transmission capacity, i.e. the density of secure successful transmissions at a rate $\log(1+\theta_{\mathrm{D}})$ as [246]:

$$\begin{aligned} \Upsilon &= \lambda_{\mathrm{D},a} \log(1+\theta_{\mathrm{D}}) \mathscr{P}\left(\gamma_{i,0} \geq \theta_{\mathrm{D}}\right) \\ &= \lambda_{\mathrm{D},a} \log(1+\theta_{\mathrm{D}}) \frac{1 - e^{-\mu_{\mathrm{r}}^2 (a_2 + a_3)}}{(a_2 + a_3) D^2}, \end{aligned} \tag{4.12}$$

where $a_2 = \left(\pi \lambda_{\mathrm{C},a} \theta_{\mathrm{D}}^{\delta} / \operatorname{sinc} \delta\right) \mathrm{E}\left[P_{\mathrm{C}}^{\delta}\right] P_D^{-\delta}$; $a_3 = \pi \lambda_{\mathrm{D},a} \theta_{\mathrm{D}}^{\delta} / \operatorname{sinc} \delta$.

4.5 Results

In this section, we present numerical results to study the achievable transmission capacity of secrecy-based D2D cellular networks with spatial spectrum sensing. Unless otherwise stated, we set the following system parameters: $R_{\mathrm{B}} = 788$ meters (which corresponds of an inter-BS distance of 1500 meters), $\zeta = 0.5$, $D = 100$ m, $\alpha = 4$, $\lambda_{\mathrm{B}} = 1/\left(\pi R_{\mathrm{B}}^2\right)$, $\theta_{\mathrm{D}} = 20$ dB, $\upsilon_s = 0.5$, $N = 5000$, and $\rho = 10^{-11}$.

Fig. 4.2 shows the average achievable secrecy transmission capacity versus λ_{U} for different values of q. As more users are operating in D2D mode (i.e., when q increases), the achievable transmission capacity becomes higher due to the receiver becoming closer in distance to the transmitter and eavesdroppers becoming far away. Moreover, as the intensity of users increases, the secrecy transmission capacity increases since the interference of a larger legitimate user population can be exploited in a beneficial way to protect D2D links from eavesdropping, from a physical layer security perspective. Fig. 4.3 shows the average achievable secrecy transmission capacity

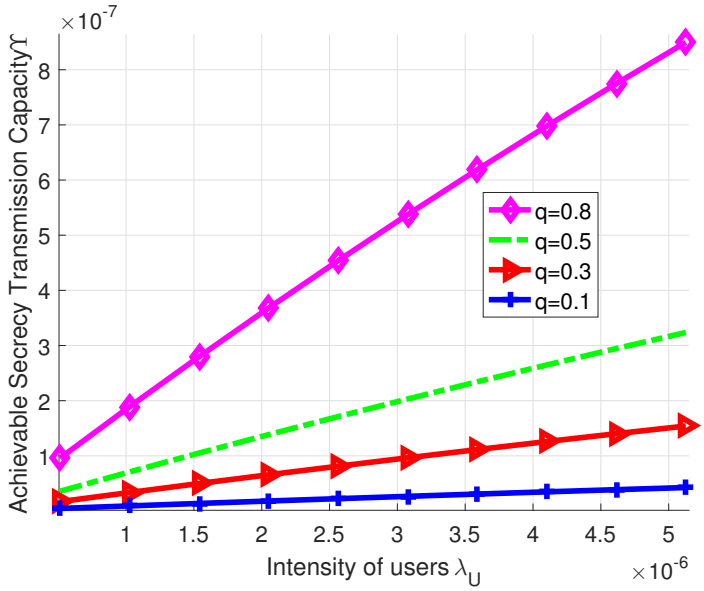

Figure 4.2: The achievable secrecy transmission capacity versus the intensity of users for different values of q ($\lambda_{\mathrm{E}} = 0.1\lambda_{\mathrm{U}}$; $R_{\mathrm{s}} = 150$ m).

versus the sensing radius R_{s} for different values of q. We see that as R_{s} increases, the spatial

sensing becomes more conservative and less aggressive. This means, the probability of detecting spatial spectrum holes decreases, leading to fewer active D2D transmissions. This in turn increases the distances between the D2D transmitters and receivers, thereby making the D2D links more susceptible to eavesdropping. That is why we see a decreasing behavior in the secrecy transmission capacity as the sensing radius increases.

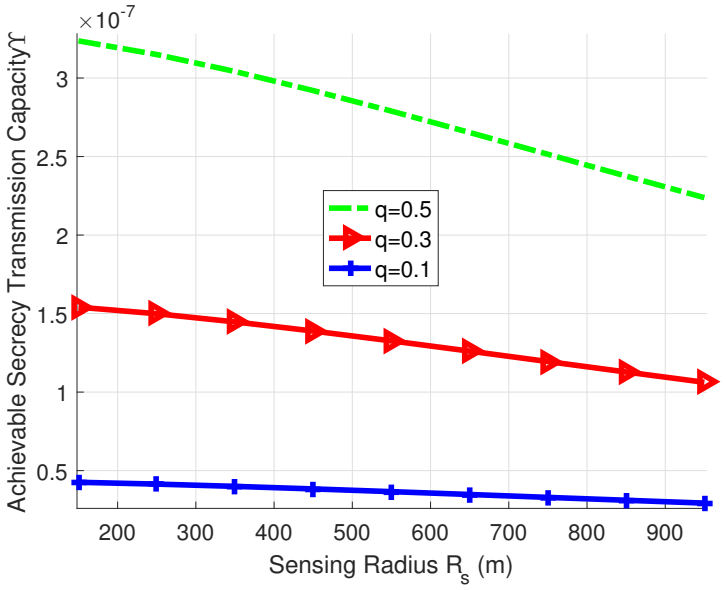

Figure 4.3: The achievable secrecy transmission capacity versus the sensing radius for different values of q ($\lambda_{\mathrm{U}} = 10\lambda_{\mathrm{B}}$ and $\lambda_{\mathrm{E}} = 0.1\lambda_{\mathrm{U}}$.

4.6 Conclusions

In this chapter, we have provided a detailed discussion and analysis on spatial spectrum sensing and its effects on the density of successful secure transmissions. We showed that more aggressive sensing can better protect D2D links against eavesdropping since more D2D users become active, which reduce the distances between them.

Chapter 5

Green Traffic Offloading for CPS over Heterogeneous Networks

5.1 Introduction

In this chapter, we present another solution to relieve network congestion from CPS traffic and increase throughput of both CPS and cellular communications. More specific, we turn towards cell shrinking and offloading, a key technology in future 5G networks. Using this potential solution, we are mainly targeting two important issues: i) enabling CPS communications over cellular networks to provide CPS with several benefits such as ubiquitous coverage, global connectivity, reliability and security; and ii) offloading a proportion of CPS traffic to small cells, which in tun increases the throughput of macrocells, and frees more network resources to other users. Using stochastic geometry, we present an analysis on CPS offloading rate and achievable throughput when small cells base stations (SCBSs) are powered by solar energy. The solar energy harvesting allows SCBSs to offset the costs of serving CPS devices. Our results show the potential benefits for both macrocells and small cells in terms of minimum achievable throughput when the CPS offloading rate is high.

In this chapter, we consider a single tier of power-grid MBSs and K tiers of SCBSs powered by solar energy harvesting. Part of the CPS communications will be offloaded to SCBSs to help relieve

cellular congestion. The uncertainty in energy harvesting can reduce the amount of offloaded data, which is why we take into consideration the unexpected change in solar power due to season, weather, or other effects. We try to answer several questions through stochastic geometry analysis and numerical results: which network metrics maximize the amount of offloaded CPS traffic onto small cells? How much gains can we obtain in the achievable throughput by offloading CPS traffic, and how does the offloading impact the achievable throughput of small cells? We summarize our contributions as follows:

- First, to the best of our knowledge, this is the first work that proposes offloading CPS communications onto energy harvesting-based small cells for purposes of supporting the anticipated massive number of CPS traffic in cellular networks, a driving force of future 5G networks.

- Second, using tools from stochastic geometry, we analytically characterize the probability of availability of SCBSs, the offloading rate, and the minimum achievable throughput of both MBS and SCBSs.

- Third, we study the impact of different network metrics on the amount of offloaded CPS traffic and achievable throughput of both macro and small cells. Our results show that the higher the SCBSs' availability is, the higher the offloading rate becomes, leading to greater benefits to small cells and macrocells in terms of minimum total achievable throughput.

The remainder of this chapter is organized as follows. In Section 5.2, a system model for a two-tier heterogeneous cellular network is presented. Section 5.3 provides expression for SCBSs availability using battery level dynamics, while Section 5.4 analytically characterizes the offloading rate and the achievable throughput of heterogeneous networks. Section 5.5 presents the numerical results and analysis. Finally, conclusions are drawn in Section 5.6.

5.2 System Model

The system model, depicted in Fig. 5.1, consists of a single tier (denoted by tier 0) of power-grid MBSs (PG-MBSs), whose locations form a homogeneous Poisson point process (HPPP) Φ_0 with density λ_0; and K tiers of solar energy harvesting SCBSs (EH-SCBSs), whose locations form an HPPP Φ_k with density λ_k, where $k \in \{1,...,K\}$. We assume that a k^{th} tier base station (BS) transmits to each of its users with fixed power P_k. The cellular users are modeled by an HPPP Φ_{c} with intensity λ_{c}. Likewise, the CPS devices are modeled by an HPPP Φ_{d} with intensity λ_{d}. Let the total number of users be $\Phi_{\text{u}} = \Phi_{\text{c}} + \Phi_{\text{d}}$ with intensity $\lambda_{\text{u}} = \lambda_{\text{c}} + \lambda_{\text{d}}$. Through stochastic geometry analysis, we are able to provide an accurate model of BSs' and users' spatial locations by averaging over all their potential topological realizations [241].

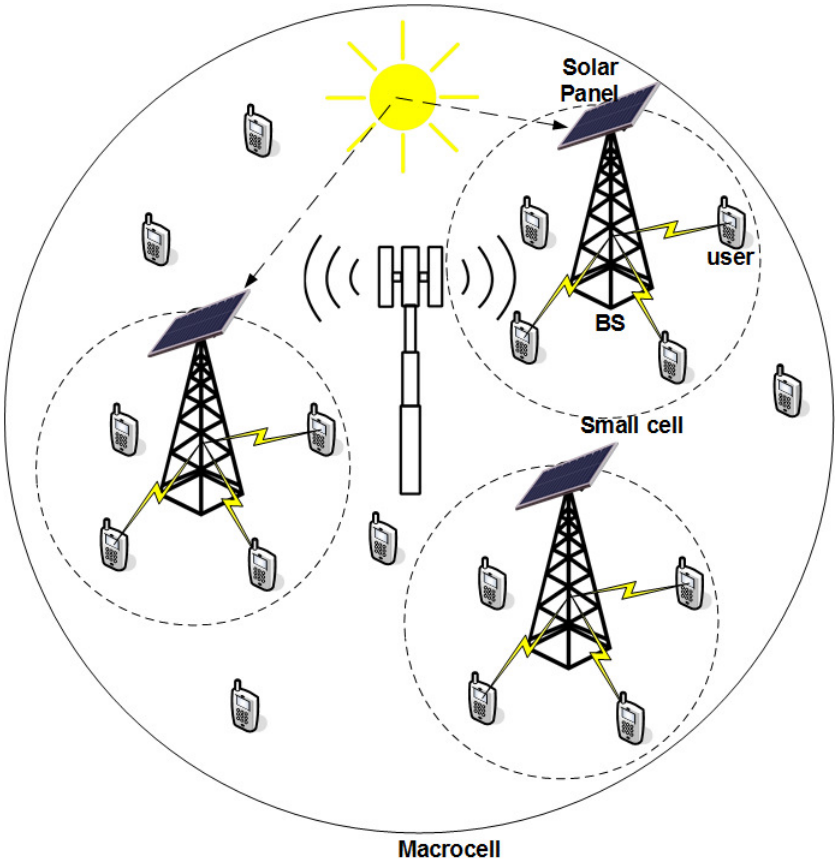

Figure 5.1: An example of a heterogeneous network powered by solar energy harvesting.

Let $\|x_k - z\|$ denotes the distance between a k^{th} tier BS located at $x_k \in \Phi_k$, $k \in \{0,..,K\}$, and

a user located at $z \in \Phi_{\mathrm{u}}$. We assume that the power of the signal transmitted by the BS decays at a rate of $\|i-j\|^{-\alpha}$, where $\alpha > 2$ is the path-loss exponent. Rayleigh fading with mean one is used to model the small-scale fading over each channel, with $h_{x_k,z}$ denoting the channel coefficient between SCBS located at x_k and a user located at z. From now on, we drop the subscripts from $h_{x_k,z}$ since it is independent of the locations of x_k and z. Since each user connects to the BS with the highest received power, we do not consider small scale fading for cell association. In addition, we adopt a biased cell association policy, where each BS of tier k has biasing factor $B_k > 0$ [248].

The service region $\mathscr{A}_k(x_k) \subset \mathbf{R}^2$ of the k^{th} tier BS located at $x_k \in \Phi_k$, with $k \in \{0,...,K\}$, is random and defined as [249]:

$$\mathscr{A}_k(x_k) = \left\{ x \in \mathbf{R}^2 : x_k = \underset{x \in x_j^\star}{\arg\max}\, P_j B_j \|x-z\|^{-\alpha}, \text{where } x_j^\star = \underset{x \in \Phi_j^\star}{\arg\max}\, P_j B_j \|x-z\|^{-\alpha} \right\}, \quad (5.1)$$

where $x_j^\star$ denotes the candidate BS with the highest average received signal power selected by user $z \in \Phi_{\mathrm{u}}$ as a serving BS.

Then, the average area of service region of k^{th} tier BS is given as [249]:

$$\mathrm{E}[|A_k|] = \frac{\tilde{\lambda}_k \left(P_k B_k\right)^{2/\alpha}}{\sum_{j=0}^{K} \tilde{\lambda}_j \left(P_j B_j\right)^{2/\alpha}}, \quad (5.2)$$

where $\tilde{\lambda}_j$ is the density of available BSs of tier j, i.e., BSs that have sufficient available energy. This will be discussed in details in Section 5.3. Eq. (5.2) can be further expressed as [250]

$$\mathrm{E}[|A_k|] = \left[\sum_{j=0}^{K} \bar{\lambda}_{jk} \left(\bar{P}_{jk} \bar{B}_{jk}\right)^{2/\alpha} \right]^{-1}, \quad (5.3)$$

where $\bar{\lambda}_{jk} \triangleq \tilde{\lambda}_j / \tilde{\lambda}_k$; $\bar{P}_{jk} \triangleq P_j / P_k$; and $\bar{B}_{jk} \triangleq B_j / B_k$. Without loss of generality, we assume a typical user at the origin using Slivniyaks theorem [251]. The aggregate interference at a typical user

serviced by a BS located at $x \in \tilde{\Phi}_k$ is:

$$I_{\text{tot},0} = \sum_{k=0}^{K} \sum_{k \in \tilde{\Phi}_k \setminus x} P_k h_k \|k\|^{-\alpha}, \tag{5.4}$$

where $\tilde{\Phi}_k$ is a PPP representing the set of available BSs that are transmitting with intensity $\tilde{\lambda}_k$. Then, the signal-to-noise-plus-interference ratio (SINR) is given by:

$$\gamma_0 = \frac{P_k h_k \|x\|^{-\alpha}}{I_{\text{tot},0}}. \tag{5.5}$$

5.3 Solar Energy Harvesting Model

In this section, we describe the solar energy harvesting model to power SCBSs.

Table 5.1: Estimated power harvested from different sources [3].

Energy Source	Harvested Power
Vibration/Motion	
Human	4μW/cm^2
Industry	100μW/cm^2
Light	
Indoor	10μW/cm^2
Outdoor	10mW/cm^2
RF	
GSM	0.1μW/cm^2
WiFi	0.001mW/cm^2

Challenges: Solar energy harvesting is very appealing since it can provide the highest energy density among the other renewable sources, as can be seen from Table 4.1, which shows the estimated power that can be harvested from different sources [3]. Note that even though solar energy harvesting has the highest energy intensity compared to other energy harvesting sources (see Table 4.1), it has many drawbacks, such as dependence on weather changing factors and geographical regions which must be taken into consideration; inability to be used in cloudy areas that have low

incidence of ambient solar irradiance; and so on. All these factors put a question mark whether solar energy harvesting is a reliable source of energy. Indeed, the uncertainty in energy harvesting can reduce the amount of offloaded data from macrocells to small cells, leading to CPS' performance deterioration. That is why, in this paper, we model the solar energy harvesting by taking into account the unexpected change in solar power due to season, weather, and other effects.

In this section, we characterize the probability that an EH-SCBS in tier $k \in \{1,..,K\}$ is available to provide services to its users. Our solar energy model is based on [252] and [253], which captures many parameters that affect the amount of solar irradiance. First, to understand what solar irradiance includes, we refer to Fig. 5.2, which shows the different components of solar irradiance. It can be thought of as the sum of the direct beam radiation that comes from the sun, the diffuse radiation that gets scattered out by objects, molecules, aerosols and clouds, and the radiation that gets reflected off the ground into the atmosphere. It is measured in Watts/meters^2. We can model

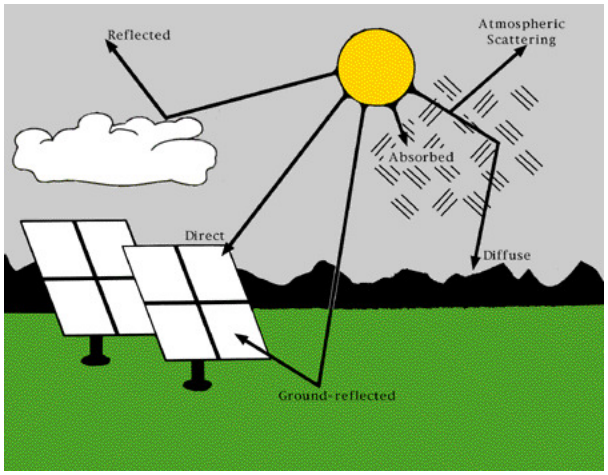

Figure 5.2: An illustration of the different components of solar irradiance (retrieved from [2]).

the average solar radiation in terms of the time of the day τ as:

$$R(\tau) = \frac{h_{\text{peak}}}{2} \cdot \left[1 + \cos\left(\frac{\pi}{6}(\tau - 12)\right)\right] + A_{\text{r}} \cdot \mathcal{N}(\tau, 1), \tag{5.6}$$

for $6 \leq \tau \leq 18$ and 0 otherwise; where h_{peak} is the peak value of the harvesting power which is a function in terms of the season or weather. $A_{\text{r}} \cdot \mathcal{N}(\tau, 1)$ captures the random changes that

can occur from cloud, rain or other effects, where A_{r} is the amplitude of the unexpected changes and $\mathcal{N}(\tau,1)$ is the Gaussian distribution with mean τ and unity variance. The amount of solar irradiance available along the path may vary depending on the shadows due to obstacles (trees, buildings, etc.), and $A_{\mathrm{r}} \cdot \mathcal{N}(\tau,1)$ captures this phenomena as well.

The harvested solar power P_{sol}^{k} for a k^{th} tier SCBS at a certain time $\tau \in \{1,\dots 24\}$ can be predicted as

$$P_{\mathrm{sol}}^{k}(\tau) = (1-L(M))e_{\mathrm{el}} \cdot e_{\mathrm{panel}} \rho A \cdot R(\tau), \tag{5.7}$$

where L is the energy loss due to inability to store solar power in the battery when temperatures are too high or too low. For example, lithium-ion batteries can neither be charged below $0^{o}C$ nor above $45^{o}C$ [253]. The solar irradiance R in (5.6) is multiplied with the solar panel size A and the angular loss ρ to get the received radiation at a specific time τ. The angular loss accounts for the non-orthogonality of solar radiation on the panel. However, only a fraction of the solar radiation can be converted into electrical power due to solar panel efficiency losses e_{panel}, as well as losses e_{el} during electrical conversion.

Let $S_{t,k}$ denotes the average battery level at time t for k^{th} tier SCBS. The dynamics of the average battery level can be captured as

$$S_{t,k} = \min\left\{ S_{t-1,k} + \varepsilon_k - P_{k,\mathrm{Tot}}(t) T \mathbb{1}_{S_{t-1,k} \geq P_{k,\mathrm{Tot}} T} \right\}, \tag{5.8}$$

where $\varepsilon_k = P_{\mathrm{sol}}^{k}(t)$; $P_{k,\mathrm{Tot}}(t) = \Delta_k P_k + P_{k,\mathrm{static}}$ is the total power consumption of k^{th} tier SCBS, with Δ_k being the slope of the load-dependent power consumption and $P_{k,\mathrm{static}}$ is the static power expenditure [254]; T is the transmission slot period; and $S_{0,k} = G$ is the initial battery capacity level identical for all SCBSs. Let v_k denotes the required number of time slots to harvest sufficient power for transmission. Denote by P_H^k the harvested power by the energy harvesting circuit in the k^{th} tier SCBS. Denote the following notations: $V = (1-L(M))e_{\mathrm{el}} \cdot e_{\mathrm{panel}} A$, and $U = (h_{\mathrm{peak}}/2) \cdot$

$\left[1+\cos\left(\frac{\pi}{6}(\tau-12)\right)\right]$, then the energy harvesting probability of k^{th} tier SCBS can be expressed as

$$\begin{aligned}\varphi_k = \mathscr{P}\left(P_H^k > \varepsilon_k v_k\right) &= \mathscr{P}\left(V\cdot U + VA_{\text{r}}\mathscr{N}(\tau,1) > \varepsilon_k v_k\right)\\ &= \mathscr{P}\left(\mathscr{N}(\tau,1) > \frac{\varepsilon_k v_k - U\cdot V}{VA_{\text{r}}}\right)\\ &= \frac{1}{2}\operatorname{erfc}\left(\frac{\varepsilon_k v_k - U\cdot V}{VA_{\text{r}}\sqrt{2}}\right),\end{aligned} \tag{5.9}$$

where $\operatorname{erfc}(z) = 1-\operatorname{erf}(z)$ is the complementary error function.

We define the availability ρ_k of k^{th} tier SCBS as [228]:

$$\rho_k = \lim_{n\to\infty}\frac{1}{n}\sum_{t=1}^{n}\mathrm{E}\left[\mathbb{1}_{S_{t,k}\geq\varepsilon_k v_k}\right]. \tag{5.10}$$

Assuming infinite batter capacity[1], according to [228], the probability of availability of k^{th} tier SCBS can be expressed as

$$\rho_k = \min\left(1, \frac{\varepsilon_k}{P_{k,Tot}}\right). \tag{5.11}$$

Thus, the density of available SCBSs forms a thinning PPP $\tilde{\Phi}_k$ from Φ_k, with intensity $\tilde{\lambda}_k = \rho_k\lambda_k$. The PG-MBSs are always available due to always having sufficient energy for transmission, then they form an HPPP $\tilde{\Phi}_0 = \Phi_0$ with intensity $\tilde{\lambda}_0 = \lambda_0$.

5.4 CPS Offloading Rate

In this section, we analytically characterize the offloading rate of CPS traffic from an MBS b to SCBS[2].

Theorem 12. *In interference-limited network (i.e., noise power is ignored, $\sigma^2 = 0$ [255]) and when all tiers have the same SIR threshold β, the probability that a typical user achieves β when*

[1]The limit of exceeding the battery capacity is negligible when the capacity is much larger than the average stored energy. Thus, the infinite battery capacity assumption can be regarded as an approximation [254].

[2]In this paper, we focus our analysis and derivations on offloading CPS traffic solely, excluding regular cellular traffic for the sake of highlighting the benefits of CPS traffic offloading.

it associates with its serving BS in k^{th} tier can be expressed as

$$P_{c,k} = \mathscr{P}(\gamma_k \geq \beta) = \exp\left(-\pi \sum_{j=0}^{K} \tilde{\lambda}_k \bar{P}_{jk}^{2/\alpha} r^{2/\alpha} \frac{2\beta \bar{B}_{jk}^{2/\alpha-1}}{\alpha-2} {}_2F_1\left(1, 1-\frac{2}{\alpha}; 2-\frac{2}{\alpha}, -\frac{\beta}{\bar{B}_{jk}}\right)\right), \tag{5.12}$$

${}_2F_1(a,b;c,z) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-tz)^{-a}dt$ is the hypergeometric function.

Proof : *See Appendix 8.5.*

Let $\lambda_{\text{b}} = \tilde{\lambda}_0$. The following lemma provides the average number of CPS devices N_b^k that are offloaded from MBS b to SCBS k.

Lemma 6. *The average number of CPS devices N_b^k that are offloaded from MBS b to SCBS k can be expressed using the mean load approximation [248]:*

$$\mathrm{E}\left[N_b^k\right] = \frac{\lambda_d}{\lambda_b} P_{c,k} \mathrm{E}[|A_k|]. \tag{5.13}$$

Theorem 13. *The offloading rate of CPS devices from MBS b to SCBSs can be characterized as*

$$\mu_b = \frac{\sum_{k=1}^{K} \mathrm{E}\left[N_b^k\right]}{\lambda_d/\lambda_b}. \tag{5.14}$$

Lemma 7. *By Shannon's theorem, the minimum achievable data rate of a typical user when it associates with a k^{th} tier SCBS can be expressed as [256]*

$$R_k = \mathrm{E}\left[\frac{W}{N_k}\log_2(1+\beta)\right] = \frac{W}{\mathrm{E}[N_k]}\log_2(1+\beta), \tag{5.15}$$

where W is the system bandwidth; and $\mathrm{E}[N_k]$ is the average number of users associated with k^{th} tier SCBS, and given as $\mathrm{E}[N_k] = \lambda_u/\tilde{\lambda}_k + \mathrm{E}\left[N_b^k\right]$.

Theorem 14. *The minimum achievable throughput of all K-tiers small cells can be characterized*

as [256]

$$
\begin{aligned}
R_{total} &= \sum_{k=1}^{K} P_{c,k}\lambda_u \mathrm{E}[|A_k|]R_k \\
&= \lambda_u W \log_2(1+\beta) \sum_{k=1}^{K} \left\{ P_{c,k} \left[\sum_{j=0}^{K} \bar{\lambda}_{jk} \left(\bar{P}_{jk} \bar{B}_{jk} \right)^{2/\alpha} \right]^{-1} \frac{1}{\lambda_u/\tilde{\lambda}_k + \mathrm{E}\left[N_b^k\right]} \right\}.
\end{aligned} \tag{5.16}
$$

Eq. (5.16) shows that the minimum achievable throughput is related to the availabilities of SCBSs, the users density, the number of users offloaded to SCBSs and the coverage probability. We study the impact of many of these metrics in the next section.

Finally, we can characterize the minimum achievable throughput of the 0-tier PG-MBSs as

$$
R_{\mathrm{total}} = P_{\mathrm{c},0}\lambda_{\mathrm{u}} W \log_2(1+\beta) \left[\sum_{j=0}^{K} \bar{\lambda}_{j0} \left(\bar{P}_{j0} \bar{B}_{j0} \right)^{2/\alpha} \right]^{-1} \frac{1}{\lambda_{\mathrm{u}}/\lambda_{\mathrm{b}} - \sum_{k=1}^{K} \mathrm{E}\left[N_{\mathrm{b}}^k\right]}. \tag{5.17}
$$

5.5 Results and Analysis

In this section, we present numerical illustrations using MATLAB simulation tool to study the amount of offloaded traffic and its impact on the minimum achievable throughput of both macrocell and small cells. Unless otherwise noted, we set the following system parameters: $\lambda_{\mathrm{u}} = 100/(\pi 1000^2)$; $\lambda_k = [0.09, 0.05, 0.01] \cdot \lambda_{\mathrm{u}}$; $\beta = 3$ dB [250]; $\lambda_{\mathrm{d}} = 0.5\lambda_{\mathrm{u}}$; $W = 20 * 10^6$ Hz [248]; $P_k = [46, 33, 23]$ dBm [257]; $B_k = [1, 10, 10]$ dB [258]; $\alpha = 4$; $K = 3$; $L(M) = 0.25$; $e_{\mathrm{el}} = 0.7$; $e_{\mathrm{panel}} = 0.07$; $\rho = 0.7$; $A = 170cm^2$ [253]; $A_{\mathrm{r}} = 0.4$; $\delta_k = 8$; $P_{k,\mathrm{static}} = 4.8$ Watt; and $T = 1$ sec [254].

Fig. 5.3 shows the offloading rate versus the probability of availability of SCBSs for different values of biasing factors. If a small cell has a biasing factor of 10 dB, it means that a macrocell user is willing to be associated with that small cell even if the received maximum power is 10 dB less than that of the macrocell. First, we see that an increase in the availability of SCBSs yields an increase in the offloading rate, since SCBSs become more willing to serve macrocell users when they have harvested enough solar power. Second, as the biasing factor increases, so does the offloading rate since CPS devices become more inclined towards associating with SCBSs. That

is, with SCBSs becoming more available and macrocell users becoming more biased to associate with these small cells, we see an increasing trend in the amount of offloaded CPS traffic. For instance, we see from Fig. 5.3 that if CPS devices are willing to associate with SCBSs if the maximum received power is 20 dB less than the macrocell, then the offloading rate can reach almost 60% provided SCBSs are highly available. It is interesting to note that with the probability of availability of SCBSs approaching 1, the offloading rate does not increase by much, but rather reaches a more stable value, especially when the SCBSs' biasing factors are high, mainly due to small cells reaching their maximum network capacity.

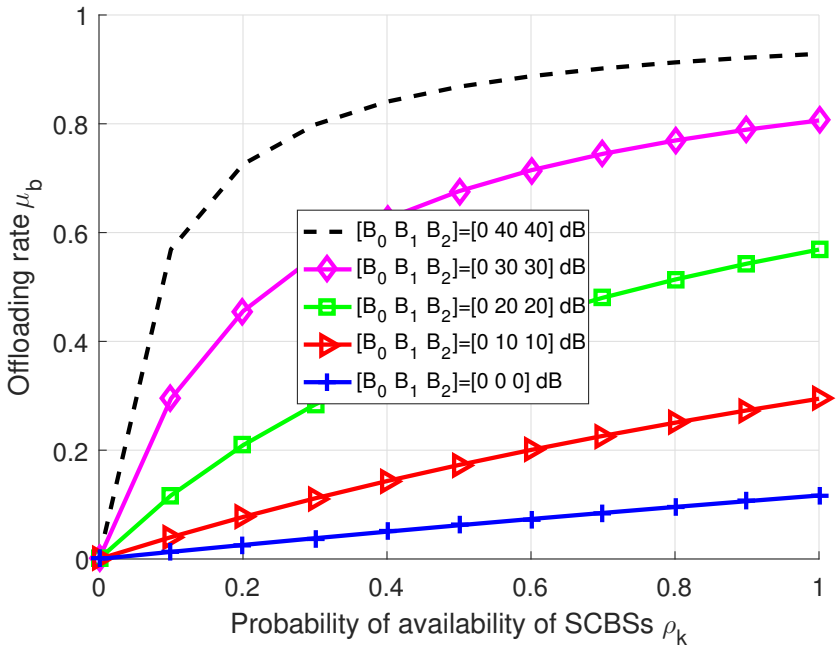

Figure 5.3: The offloading rate versus the probability of availability ρ_k of SCBS for different values of biases.

Fig. 5.4 shows the minimum achievable throughput of all K-tiers small cells versus the intensity of CPS devices λ_d for different values of biasing factors. As the intensity of CPS devices increases, the achievable throughput decreases due to the high levels of interference from a larger population of CPS devices. What is interesting to note is that as the biasing factor towards SCBSs increases, the total throughput of users increases, since more users get offloaded from macrocell to small

cells, which have higher throughout due to shorter distances and users being closer to the SCBSs. Furthermore, small cell users have lower mobility than macrocell users leading to less fading and high capacity.

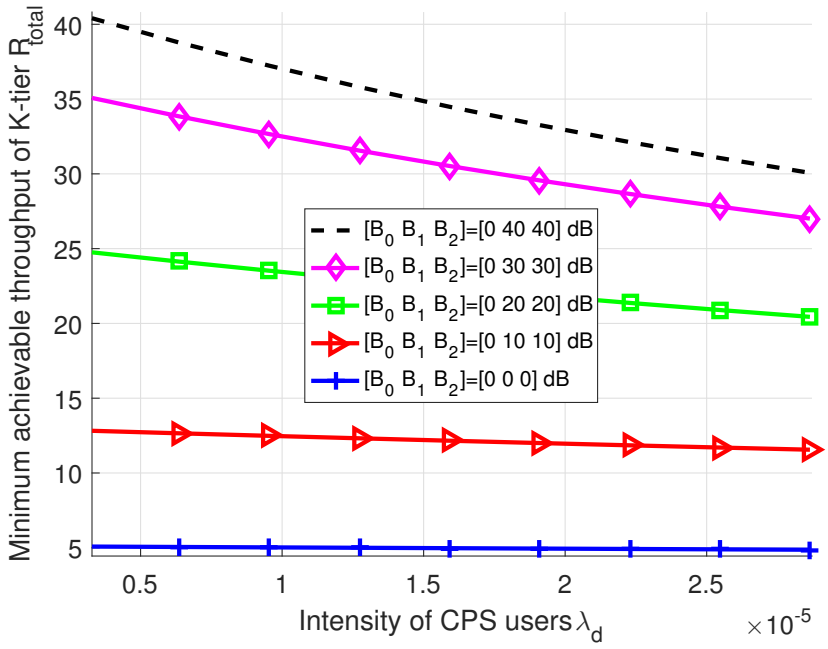

Figure 5.4: The minimum achievable throughput of all K-tiers small cells versus the intensity of CPS devices λ_d for different values of biases.

Finally, Fig. 5.5 shows the minimum achievable throughput of the 0-tier macrocell versus the he probability of availability ρ_k of SCBS for different values of CPS intensity λ_d. It is clear that when SCBSs become more available, the macrocell experiences higher throughput since more CPS users get offloaded to SCBSs, thereby freeing more network resources to other macrocell users. Moreover, in the presence of a large number of CPS users, a large proportion of them get offloaded to small cells, leading to even higher total achievable throughput for the macrocell.

5.6 Conclusion

In this chapter, we have presented a potential solution to the anticipated massive number of CPS devices that will be expected to communicate over the cellular spectrum. Using the concept of

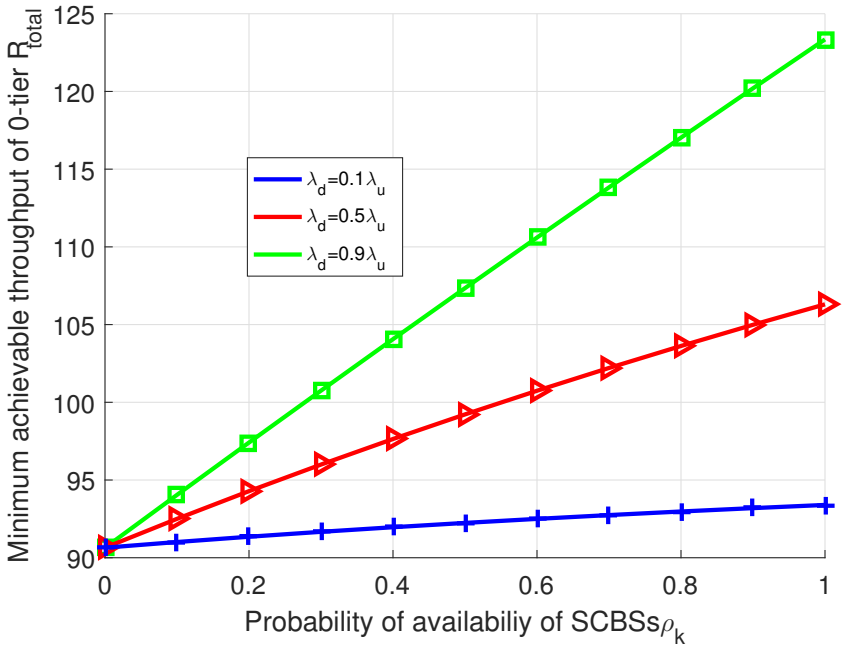

Figure 5.5: The minimum achievable throughput of the 0-tier macrocell versus the he probability of availability ρ_k of SCBS for different values of CPS intensity λ_d.

cell shrinking and offloading technology, a proportion of CPS communications are offloaded from macrocell to small cells. We allowed SCBSs to be powered by solar power to offset the costs of serving CPS devices. In other words, as long as SCBSs are available (i.e., they have enough available power), the CPS traffic offloading can bring benefits to both macrocell BSs and SCBSs. Indeed, we showed in our results that a high biasing factor and a high availability probability of SCBSs can lead to a high CPS offloading rate and a high minimum achievable throughout for the macrocell as well as for the small cells.

Chapter 6

A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems

6.1 Introduction

Mobile Health (m-Health) has recently grown in popularity due to its ability to improve patients' health status by delivering efficient, effective and high-quality healthcare. Different from e-Health systems that are targeted for small-scale networks using wearable biomedical sensors, the Internet, and other related technologies such as virtual reality in prevention, diagnosis and treatment, m-Health systems are emerged as next-generation e-health systems where mobile devices, wireless technologies, and social media have made possible the storage, processing, and analysis of large volume of data as well as remote sensing for long-term continuous health monitoring [195, 90, 259]. M-health systems will shape the future of tele-medicine across multiple disciplines from cardiology, surgery to psychiatry, especially with their continuous expansion. It is expected that by 2020, there will be more than 774 million connected health-related devices [90].

The last decade has witnessed technological advancements in the healthcare system through the use of wireless biomedical sensors by deploying a medical body area network (MBAN). In an MBAN, sensors are placed in the vicinity of patient's body or even inside the body to collect health-

related data using short-range wireless technologies. The collected data is then transmitted to the medical staff who analyzes them for purposes of monitoring patients' physiological conditions and disease progression in a cost-effective way. Unlike conventional wire-connected devices that limit patient's mobility, the use of wireless sensors on human body provides greater mobility and comfort. Some potential m-Health applications include diabetes management by measuring blood sugar levels and the insulin dosage, blood pressure and heart rhythm monitoring, elderly support by tracking their medications and activity levels, fitness indicators monitoring during workouts, and a myriad of other applications [90].

The use of mobile communications allows the healthcare practitioners to use the sensed vitals signs (electrocardiogram, oxygen saturation, glucose level, etc.) together with patient's medical history to remotely control the medications, intensity of exercises, detect a life-threatening state, etc. This means that these vital signs need to be reliably, timely and securely transmitted to the remote medical location [260]. This constitutes a potential cyber-physical systems (CPS) application in healthcare, where a CPS is defined as a system with integrated communication and computational capabilities with tight interactions with the physical world [261]. In the context of healthcare, the various biomedical sensors and the mobile devices that interact with each other constitute the physical world, which needs to convey the processed vital signs to an m-Health server running monitoring programs for patients with chronic diseases [261, 195].

With m-Health being employed on a large scale with tight intensive interactions among its sensors and mobile devices, it creates a set of challenges, among which the security and privacy of patients' personal health information (PHI) are the most important ones [262]. These security vulnerabilities are made easy with the nature of the open wireless medium, which introduces eavesdropping, data fabrication and privacy violation threats. As a matter of fact, an eavesdropper can intercept the communication between the sensors and the mobile devices in an attempt to steal or fabricate patients' PHI. By doing so, the eavesdropper can guess the patient's disease or health status with high probability.

In this chapter, we consider a three-tier m-Health architecture, adopted in [263, 264, 260, 265].

The first tier is the sensor network tier where sensors on the body or around the residence of the patient capture vital signals using a short range wireless technology such as Bluetooth. The sensed data is then transmitted to the mobile computing network tier, where mobile devices form an ad-hoc network to route the data to a fixed remote location. Finally, the back-end network tier consists of servers with high computational capabilities that analyze the sensed data along with patient's past medical records and transmit a medical report to the medical staff. To provide privacy protection for patient's data records, we aim to develop a physical layer security scheme by exploiting the characteristics of wireless channels in the second tier, mainly because it is more vulnerable to security threats due to i) the limited computational capabilities of mobile device to employ data confidentiality, privacy preservation and authentication; ii) the semi- or fully-autonomous security management (mutual authentication, key arrangement, etc.) [194]; and iii) the high computational overhead cost of cryptography in mobile health applications [195]. This work can be easily extended to include privacy protection in the first tier; however it is out of the scope of this chapter.

6.1.1 Related Work

While cryptography can guarantee to some extent the data confidentiality, integrity and authentication [37], implementing it in mobile health applications can be time consuming and costly in terms of computational overhead, high power consumption as well as the complexity of key management [38, 39]. For these reasons, we turn towards a lightweight low-complexity approach to protect the privacy of medical data measured by the sensors and processed and routed by the mobile devices by exploiting the physical characteristics of the wireless channels. This idea is not new as it dates back several centuries, where intentional echoes were generated by the circular shape of the Hall Pompeiana of Massimo in Italy in order to make its center indecipherable [40]. The work of exploiting the characteristics of wireless channels dates back to the pioneer work of Shannon and Wyner's wire-tap channel [266].

A public key infrastructure for secure healthcare in hospitals was proposed in [267]. The base station generates keys to secure the connection between itself and the patients or a healthcare

service system (HSS) through bilateral key handshaking method. Secure communication between patients and HSS can be established through using a secret key disclosed to either of them by the base station.

Patients monitoring is envisioned to reduce medical costs, allowing for more flexibility and mobility in health management while providing accurate treatment and diagnosis. A smart mobile device capable of providing continuous long-term health monitoring in a private and personalized way was proposed in [268]. To guarantee privacy protection, new patients register through the server of preferences, which generates cryptographic keys as well alarm states conditions to easily help and find lost patients.

A three-tier hierarchical healthcare architecture was proposed in [264] where different security schemes were proposed in the different tiers using public key cryptography, key agreement with a third party, a secure ad-hoc routing protocol and polynomial-based encryption. Other cryptographic solutions were also suggested in [39, 269].

Secure neighborhood discovery (ND) for users in close proximity to each other is not new and has been thoroughly investigated in literature. In addition to the use of cryptography in ND protocols, other approaches exist such as distance bounding where the distance to a potential neighbor is estimated by multiplying the signal round-trip time with its propagation speed [270]. Different works proposed different approaches to prevent measurement falsification by a dishonest user, such as [271] that used rapid bit exchange phase to measure processing and transmission delays in order to obtain a ranging distance estimate. Others suggested adding a timestamp at the appropriate instant for the outgoing messages [272]. Moreover, directional antennas approach has been proposed to detect relay attacks by using non-overlapping opposite zones to discover neighbors [273]. RF fingerprinting is another physical layer security approach that was proposed to recognize a legitimate user from an attacker by identifying the signal patterns and characteristics of the received signals [274]. Optimal power allocation to maximize the achievable secrecy rate has been investigated in [275, 276, 277] and others. Unlike the previous works mentioned, the proposed security model in this chapter is completely new and promising research frontier, which uses stochastic

geometry tools to provide insights on a transmission region that guarantees a secrecy rate and outage constraints, along with power tuning and adjustments depending on ambient interference to secure the health sensed data as they hop from one mobile device to another to reach the medical servers. Even though the research on physical layer security in healthcare systems is very limited, we provide briefly some of the previous works proposed for cellular and sensor networks.

In our prior works [278, 279], we have proposed physical layer security schemes for device-to-device (D2D) and e-health networks using similar security concepts as in this chapter. We showed in [278] that a large cellular population can be exploited in a beneficial way to protect D2D links against eavesdropping. While in [279], we optimized the privacy-protected transmission region for inter-MBAN, which allows the transmitter to adapt its power to be protected from potential eavesdroppers. In D2D cellular networks, several chapters have focused on the secure communications of cellular users in D2D-enabled networks such as [280], where the interference from D2D transmitters can jam the eavesdroppers to protect the security of cellular links. In [281], a downlink transmission was made secure in cellular network using linear precoding with regularized channel inversion. In cognitive networks, secrecy beamforming and artificial noise were shown to enhance the secure transmission of large scale spectrum sharing networks [282]. In cooperative networks, relays' trustworthiness and reputation play an important role in system performance. A relay with malicious behavior can fabricate, alter or steal the data before transmitting it. This has been investigated in many works such as [283, 284]. Finally, physical layer security schemes in wireless sensor networks have been proposed in different works [285, 286]. For instance, in [285], using stochastic geometry, the authors derived expressions for the average secrecy rate between sensors and access points and between the access points and the sinks. It was shown that multiple antennas at the access points can enhance the overall average secrecy rate of the sensor network.

6.1.2 Approach, Contributions and Organization

In this chapter, we consider a three-tier m-Health hierarchical architecture: i) sensor network tier, ii) mobile computing network tier, and iii) back-end network tier. To guarantee the privacy and

security of a large volume of health records transmitted by sensors and processed and routed by mobile devices to the servers, we propose a security scheme in the second tier using stochastic geometry. This work provides a theoretical physical layer security capacity analysis, and thus is different from security attack modeling works such as in [287, 288], in which the system is analyzed to detect, locate and deter data injection attacks. We summarize the contributions of this chapter as follows:

- First, we consider two different scenarios: when the mobile device transmits either to the nearest neighbor or to the furthest neighbor. This allows us to study the trade-off between secrecy and latency for these two scenarios through numerical illustrations, where we show that transmitting to the nearest neighbor does not necessarily result in higher latency (due to increasing the number of hops to the destination) since the probability of successful transmission in the nearest neighbor case is higher than that of the furthest neighbor case.

- Second, we characterize the transmission region around a transmitter that satisfies a specified secrecy probability, a target outage probability and a delay threshold constraint by considering two different scenarios: when the mobile devices have full information on the eavesdroppers[1], and when no information is available about the behaviors of users, i.e., whether they are legitimate users or not. In each of these scenarios, the mobile device can choose the next-hop user in its transmission region as: i) the nearest to it or ii) the furthest to it.

- Third, the analytical framework allows us to compare different performance metrics such as the transmission region and the average end-to-end delay for the different scenarios under study.

The remainder of this chapter is organized as follows. In Section 6.2, a system model for a three-tier hierarchical m-Health system with eavesdroppers overhearing the mobile devices' communications is presented. Section 6.3.1 presents the coverage analysis of mobile computing tier.

[1]In this chapter, the eavesdroppers are non-legitimate users whose locations in the hospital follow a homogeneous Poisson point process.

The secrecy of mobile links is analyzed for two different scenarios: when having full information on eavesdroppers, and when that information is not available in Section 6.3.2 and Section 6.3.3; respectively. Section 6.3.4 presents the average end-to-end delay analysis. Section 6.4 presents the numerical illustrations and analysis. Finally, conclusions are drawn in Section 6.5.

6.2 System Model

6.2.1 M-Health Model

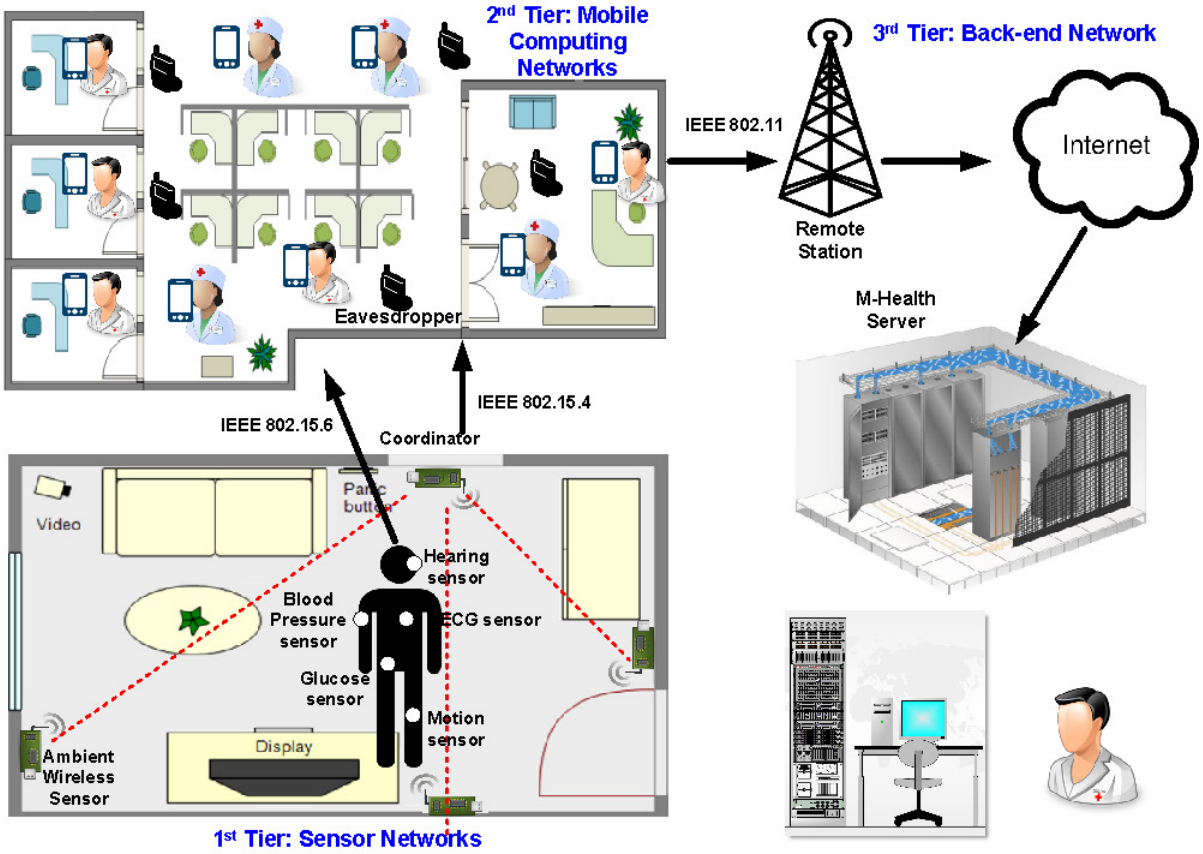

Figure 6.1: An example of a three tier hierarchical m-Health system in presence of multiple eavesdroppers.

Fig. 6.1 shows a three tier m-Health network architecture: sensor network, mobile computing network, and back-end network, along with a set of eavesdroppers overhearing the communication

of the mobile computing network tier. All nodes in the first and second tiers share the same unlicensed ISM (Industrial, Scientific and Medical) band. The sensor network communication refers to communication between medical biosensors, which collect health-related data such as blood pressure, insulin level, heart rhythm, etc. from patient's own body, and transmit them to the second network tier. The sensors can be either placed on patient's body (MBAN) using the IEEE 802.15.6 standard for on-body communications; and/or in the patient's surroundings (e.g., in the patient's home or in a nursing house) forming a ZigBee network using the IEEE 802.15.4 standard for physical and medium access control (MAC) layer communications. The sensors should transmit at a low power since they are operating at close proximity from the body. This helps extend their battery lifetime and reduce the dangers of electromagnetic radiation exposure on the patient [289]. The second tier consists of mobile devices such as PDA and laptop organized in an ad-hoc network. These mobile devices need to support multiple network interfaces: Bluetooth and ZigBee to communicate with the lower tier and WLAN for communication with the upper layer. The sensed data is then routed through the mobile ad-hoc network to reach a fixed remote or local station in the third tier that is structured on the Internet, where servers and application databases can do long-term storage, processing and analysis on the big data in order to provide a medical report on patient's health or health records access to healthcare providers [264]. It should be noted that in this paper, we are not evaluating the whole system performance, but rather the second tier's secrecy performance. We are more concerned about the security in the second tier rather than the first tier (medical sensor network), since in the latter, i) the distances between sensors are very short unlike the second tier, and ii) the security of the collected sensed data at the coordinator cluster head is more significant than the individual sensed data by medical sensors.

In what follows, we describe the model of the second tier network for which we develop a security scheme, using stochastic geometry. Stochastic geometry provides an accurate model of interferers' spatial locations by averaging over all their potential topological realizations [290]. With nodes sharing the unlicensed bands, stochastic geometry takes into consideration not only the channel model, but also the MAC to determine concurrently transmitting nodes' spatial distri-

bution, i.e., the effective interferers [291].

6.2.2 Sensor and Mobile Computing Tier Networks Model

We consider that the sensor network tier consists of sensors in the patient's environment communicating with a coordinator (CN) using the IEEE 802.15.4 wireless personal area networks (WPANs), and sensors placed on patient's body or inside her collecting data using the IEEE 802.15.6 standard. The IEEE 802.15.4 standard defines the physical and link layers for low data rate communications, on which ZigBee standard is built on top to provide upper layer communications; while the IEEE 802.15.6 standard is dedicated for short range wireless communications in the vicinity or inside the human body using low transmission power. On the other hand, the mobile computing tier uses the IEEE 802.11 ad-hoc mode standard for communication. This standard provides a low-cost technology with high coverage and throughput, making it suitable to set up a mobile ad-hoc network (MANET) [292]. Unlike IEEE 802.15.4, IEEE 802.11 nodes operate at higher transmission power (30 dBm) with higher data rates [293]. This creates coexistence problems between IEEE 802.11 and IEEE 802.15.4/802.15.6, especially that there is a significant overlap between most of the channels used by these standards. As for channel access, all these networks use the carrier sense multiple access with collision avoidance (CSMA/CA), allowing multiple nodes to transmit at different times without interference.

6.2.3 Channel Model

The distance between any two nodes i and j is denoted by $\|i-j\|$. We assume that the power of the signal transmitted by nodes decays at a rate of $l(i,j) = \|i-j\|^{-\alpha}$, where $\alpha > 2$ is the path-loss exponent of transmitters. We use Rayleigh fading with mean one to model the small-scale fading over each channel. Let h_{ij} denotes the channel coefficient between nodes i and j. Let $P_{\text{MBAN},i}$, $P_{\text{CN},i}$, and $P_{\text{MANET},i}$ denote the powers of i^{th} MBAN sensor node, i^{th} CN node, and i^{th} 802.11 mobile node, respectively.

For reliable communication, we assume that all users use a truncated channel inversion power

control [213, 294] to assure that the average received signal power at the intended receiver is at least equal to its sensitivity. Let L_{m} be a random variable representing the link length of a typical node. Thus, nodes will use power control $P_i = \rho L_{\mathrm{m}}^{\alpha}$; and $\rho \ll 1$ denotes the coefficient of proportionality that scales down the actual transmit power since in reality, the practical transmit power of a node is far less than the path-loss [1].

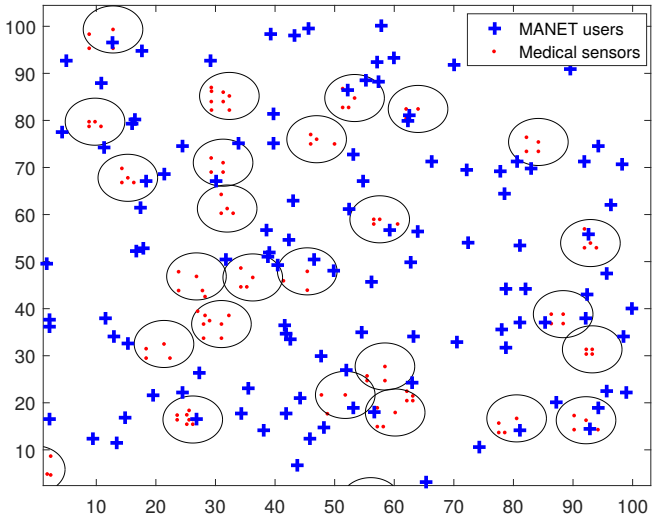

Figure 6.2: A topological realization of an m-Health system with medical sensor and MANET networks.

6.2.4 Interference Sources

In what follows, we consider the Euclidean plane $\mathbb{R}^2$. Fig. 6.2 shows a topological realization of medical sensor and MANET networks. The MBAN sensor nodes' spatial locations follow a homogeneous Poisson point process (PPP), $\Phi_{\mathrm{MBAN}}(t)$ of intensity $\lambda_{\mathrm{MBAN}}(t)$ at some instant time t[291]. In what follows, the index t will be omitted to simplify the notations. Since the channel of MBAN is divided into superframes containing active and inactive periods, we therefore model the active MBAN sensor nodes as a thinning PPP, $\Phi^{\mathrm{a}}_{\mathrm{MBAN}}$ of intensity $\lambda^{\mathrm{a}}_{\mathrm{MBAN}} = \eta\lambda_{\mathrm{MBAN}}$, where η is the duty cycle of an MBAN sensor node representing the percentage of period activity in a superframe [291]. The spatial locations of the CNs in IEEE 802.15.4 are modeled according to a

homogeneous PPP, Φ_{CN} with intensity λ_{CN} [295]. Furthermore, IEEE 802.11 transmitters' spatial locations follow a homogeneous PPP, Φ_{MANET} of intensity λ_{MANET}. The receivers are assumed to be located randomly around the transmitters, i.e., they can be present anywhere within a given region [296]. We assume that all nodes employ contention-based channel access and use CSMA/CA where a node transmits only if no other nodes are detected active within a sensing range. A node is continuously sensing the medium. If it detects another node in its contention domain, it refrains from transmitting and freezes its timer. The timer specifies the number of time slots the node has to back-off and wait before attempting to transmit [90].

To capture the effects of CSMA/CA and to accurately model the spatial distributions of nodes, we use the Matérn hard core point process (MHCPP) type II, where each node is associated with a random independent mark uniformly distributed between $[0,1]$, and a node refrains from transmission only if there exists another node in its contention domain with a smaller mark. On the other hand, in MHCPP type I, all nodes with a neighbor in its contention domain are silenced [297]. The MHCPP type II is constructed from the parent PPP, which represents the set of all contending nodes. We define the contention domain as a random shaped region depending on the channel fading, where nodes continuously sense the medium, measure the power level and then compare it to a carrier sensing threshold δ. If the measured power is less than δ, the nodes can transmit; otherwise they back off.

The intensity of mobile devices that access the same logical channel is given as [295]

$$\lambda^{\text{C}}_{\text{MANET}} = \lambda_{\text{MANET}} \left(1 - e^{-\mathscr{N}(\gamma)}\right) / \mathscr{N}(\gamma), \tag{6.1}$$

where $\mathscr{N}(\gamma) = \pi \lambda_{\text{MANET}} \text{E}\left[P_{\text{MANET}}^{\frac{2}{\alpha}}\right] \Gamma\left(1+\frac{2}{\alpha}\right) \delta^{-\frac{2}{\alpha}}$ represents the mean number of mobile devices in the contention domain of a generic mobile device located at $x \in \mathbb{R}^2$. Due to the rapid dynamic channel gain variations, the representative or typical mobile device cannot guarantee non-interference from other nodes in the different realizations of its contention domain. Thus,

the representative mobile device can only avoid the interference in the contention domain realized at the time it listens to the spectrum and schedules its transmission [295]. This means that the interferers no longer form an MHCPP, but rather a non-homogeneous PPP, $\Phi_{\mathrm{I}}^{\mathrm{MANET}}$ of intensity $\lambda_{\mathrm{I}}^{\mathrm{MANET}}$. The interference at a test node is generated from nodes trying to access the same channel and nodes located outside the test node's contention domain. Let $\mathscr{I}(r)$ denotes the set of interferers outside the test node's contention domain and located at distance r away from it. Then, $\mathscr{I}(r) = F_h(\delta r^{\alpha}/\mathrm{E}[P_{\mathrm{CN}}])F_h(\delta r^{\alpha}/\mathrm{E}[P_{\mathrm{MANET}}])F_h(\delta r^{\alpha}/\mathrm{E}[P_{\mathrm{MBAN}}])$, where $F_h(.)$ is the cumulative distribution function (CDF) of the channel gains [295]. Finally, $\lambda_{\mathrm{I}}^{\mathrm{MANET}} = \lambda_{\mathrm{MANET}}^{\mathrm{C}}\mathscr{I}(r)$.

6.3 Physical Layer Security Scheme

6.3.1 Coverage Analysis of Mobile Computing Tier

Without loss of generality, we consider a typical route since the mobile devices have a homogeneous distribution [298]. Therefore the subsequent analysis will be focused on a typical link along a typical route. We define the probability of a successful transmission from the typical mobile device o located at $x_o \in \mathbb{R}^2$ in the MANET using IEEE 802.11 ad-hoc mode standard to its neighbor i as: $p_{\mathrm{s}} = \mathscr{P}(\gamma_{i,o} \geq \theta)$[2], where γ denotes the signal-to-interference plus noise ratio (SINR). Since security and latency are the utmost performance metrics in m-Health CPS, we obtain p_s under two different scenarios: when the typical mobile device transmits i) to its nearest neighbor and ii) to its furthest neighbor.

We assume that the neighboring node for the typical transmitter lies within an angle $0 < \phi \leq \pi/2$ of the source-destination axis [299]. The probability density function of the distance L_{f} from any node to its furthest neighbor within $d_{\max}$ is given as [299]:

$$f_{L_{\mathrm{f}}}(r) = \frac{r\phi e^{r^2\phi/2}}{e^{d_{\max}^2\phi/2} - 1}, \qquad 0 \leq r \leq d_{\max}. \tag{6.2}$$

[2]The probability of successful transmission accross every typical link along the typical route is the same in the network [298].

On the other hand, the probability density function of the distance L_c from any node to its nearest neighbor is given as [299]:

$$f_{L_c}(r) = r\lambda\phi e^{-\lambda r^2\phi/2}, \qquad r \in \mathbb{R}^+. \tag{6.3}$$

Lemma 8. *The Laplace transform of the aggregate interference at the typical mobile device o, I_o, is given by:*

$$\begin{aligned}\mathscr{L}_{\mathscr{I}_o}(s) = \exp\Bigg(&\frac{-2\pi\lambda_I^{MANET}\mathrm{E}[P_{MANET}^{\frac{2}{\alpha}}]}{\alpha\delta^{\frac{2}{\alpha}}}\int_0^\infty \frac{s\delta x^{\frac{2}{\alpha}-1}}{s\delta+x}\left(1-e^{-x}\right)dx \\ &\cdot\int_0^\infty \frac{s\delta y^{\frac{2}{\alpha}-1}}{s\delta+y}\left(1-e^{-y}\right)dy\int_0^\infty \frac{s\delta z^{\frac{2}{\alpha}-1}}{s\delta+z}\left(1-e^{-z}\right)dz\Bigg),\end{aligned} \tag{6.4}$$

where $x = \delta r^\alpha/\mathrm{E}[P_{CN}]$; $y = \delta r^\alpha/\mathrm{E}[P_{MANET}]$; and $z = \delta r^\alpha/\mathrm{E}[P_{MBAN}]$.

Proof : *See Appendix 8.6.*

Looking at Eq. (6.4), it is very hard to use it as is for further analysis and computations. However, using numerical evaluations we can obtain explicit expressions by considering that the density of colliding nodes can be expressed as: $\tilde{\lambda}_\mathrm{k} = N_\mathrm{k}\lambda_\mathrm{k}$, with N_k being the average number of colliding nodes [300], and $\mathrm{k} = \{\mathrm{MANET,CN,MBAN}\}$. Therefore, the density of interfering nodes becomes: $\lambda_\mathrm{I}^\mathrm{k} = \lambda_\mathrm{k}^\mathrm{C}\tilde{\lambda}_\mathrm{k}$. Thus, we can re-express $\mathscr{L}_{I_o}(s)$ as:

$$\mathscr{L}_{I_\mathrm{o}}(s) = \exp\left(-\frac{\Omega\pi s^{\frac{2}{\alpha}}}{\mathrm{sinc}\left(\frac{2}{\alpha}\right)}\right), \tag{6.5}$$

where $\Omega = \lambda_\mathrm{I}^\mathrm{CN}\mathrm{E}\left[P_\mathrm{CN}^{\frac{2}{\alpha}}\right] + \lambda_\mathrm{I}^\mathrm{a,MBAN}\mathrm{E}\left[P_\mathrm{MBAN}^{\frac{2}{\alpha}}\right] + \lambda_\mathrm{I}^\mathrm{MANET}\mathrm{E}\left[P_\mathrm{MANET}^{\frac{2}{\alpha}}\right]$.

Theorem 15. *For the mobile computing tier and in interference-limited regime, the probability of*

a successful transmission $p_s = \mathscr{P}(\gamma_{i,0} \geq \theta)$ *from a typical mobile device to its neighbor is:*

$$p_s = \int_0^{\mu_c} \exp\left(-\pi\theta^{\frac{2}{\alpha}} r^2 \Omega \mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1} \mathrm{sinc}^{-1}\left(\frac{2}{\alpha}\right)\right) f_{L_m}(r)dr, \tag{6.6}$$

where μ_c *is the maximum coverage distance of the transmitter and m is c for nearest neighbor and f for furthest neighbor.*

When transmitting to the furthest neighbor, p_s *becomes:*

$$p_s = \frac{\phi\left(1 - e^{\mu_c^2\left(\phi/2 - \pi\theta^{\frac{2}{\alpha}}\mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}\right)}\right)}{2\left(\pi\theta^{\frac{2}{\alpha}}\mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega} - \phi/2\right)\left(e^{d_{max}^2\phi/2} - 1\right)}, \tag{6.7}$$

where $\tilde{\Omega} = \Omega/\mathrm{sinc}(2/\alpha)$.

When transmitting to the nearest neighbor, p_s *becomes:*

$$p_s = \frac{(\lambda_{MANET}\phi)\left(1 - e^{-\mu_c^2\left(\pi\theta^{\frac{2}{\alpha}}\mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega} + \lambda_{MANET}\phi/2\right)}\right)}{2\left(\pi\theta^{\frac{2}{\alpha}}\mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega} + \lambda_{MANET}\phi/2\right)}. \tag{6.8}$$

Proof : *See Appendix 8.7.*

Next, we obtain an upper bound on the distance μ_c that guarantees a target outage probability ν.

Corollary 1. *An upper bound for the typical link transmission success probability when transmit-*

ting to the furthest neighbor can be obtained as:

$$p_s \geq 1-\nu$$

$$\frac{\phi\left(1-e^{\mu_c^2\left(\phi/2-\pi\theta^{\frac{2}{\alpha}}\mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}\right)}\right)}{2\left(\pi\theta^{\frac{2}{\alpha}}\mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}-\phi/2\right)\left(e^{d_{max}^2\phi/2}-1\right)} \geq 1-\nu$$

$$\Rightarrow e^{\mu_c^2\left(\phi/2-\pi\theta^{\frac{2}{\alpha}}\mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}\right)} < \underbrace{1-2\phi^{-1}(1-\nu)\left(\pi\theta^{\frac{2}{\alpha}}\mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}-\phi/2\right)\left(e^{d_{max}^2\phi/2}-1\right)}_{\psi}$$

$$\Rightarrow \mu_c < \sqrt{\frac{\log\psi}{\phi/2-\pi\theta^{\frac{2}{\alpha}}\mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}}} \leq d_{max}. \tag{6.9}$$

Corollary 2. *Performing similar calculations as above gives us a lower bound on μ_c for the nearest neighbor case. Therefore, it is not straightforward to obtain an upper bound for the typical link transmission success probability when transmitting to the nearest neighbor. By applying Jensen's Inequality, we obtain a lower bound on p_s, which we then use to obtain an upper bound on μ_c. Thus,*

$$\mu_c < \frac{1}{\sqrt{\lambda_{MANET}\phi/2}}\sqrt[4]{1-\frac{2}{\alpha!}\left[\Gamma\left(\frac{\alpha}{2}+1\right)-\left(\frac{(\lambda_{MANET}\phi/2)\log(1-\nu)}{\pi\theta^{\frac{2}{\alpha}}\mathrm{E}\left[P_{MANET}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}}\right)^{\frac{\alpha}{2}}\right]}, \tag{6.10}$$

where $\Gamma(a)=\int_0^\infty e^{-t}t^{a-1}dt$.

Proof: See Appendix 8.8.

In what follows, we consider non-colliding eavesdroppers and we model their locations using homogeneous PPP, Φ_{E}, with intensity λ_{E}. The eavesdroppers attempt to intercept the transmitted

data by the mobile devices in the second tier network.

6.3.2 Full Information on Eavesdroppers

In this scenario, we assume that eavesdropper users and their spatial locations are known to the legitimate users [301, 302][3]. Recognizing legitimate users from malicious ones is out of the scope of this paper; however the process can be achieved by assigning trust values to neighbors, which are then kept in a database. Over time, the trust values are updated based on observations of users' behaviors [303]. In [304], Liu *et al.* describe different methods to estimate eavesdroppers' locations using received signal strength (RSS), angle of arrival (AOA), time of arrival (TOA), and/or time difference of arrival (TDOA). We are interested in the eavesdropper that dominates the secrecy rate, i.e., the most detrimental eavesdropper with the highest SINR. The aggregate interference at a typical eavesdropper located at a distance $\|z\|$ away from the typical mobile link is the interference generated from all users in the first and second tiers, and is given by by Eq. (6.5), since shifting the coordinates of the eavesdropper to the origin does not change the distribution of PPP [305].

Let $\max_{e\in\Phi_{\mathrm{E}}} \gamma_{e,0}$ denotes the highest received eavesdropper SINR of the typical mobile device signal, i.e., the eavesdropper with the most detrimental effect on the typical mobile device signal.

Lemma 9. *In interference-limited networks, the average probability that a mobile device link is secure is equal to the average probability that the rate of the most detrimental eavesdropper falls below a threshold ε. It is expressed as:*

$$\begin{aligned}\xi(\varepsilon) &= \mathscr{P}\left(\log\left(1+\max_{e\in\Phi_E}\gamma_{e,0}\right)<\varepsilon\right)\\ &= \exp\left(-\frac{\lambda_E}{(2^{\varepsilon}-1)^{\frac{2}{\alpha}}\,\mathrm{E}\left[P_E^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}}\right).\end{aligned} \tag{6.11}$$

[3]The secrecy of the communication can be guaranteed when the locations of eavesdroppers are known, which helps enhance the physical layer security scheme.

Proof : *See Appendix 8.9.*

Remarks : From Eq. (6.11), it is interesting to see that the average secrecy rate increases with a decrease in the eavesdroppers population, since it increases the distances of eavesdroppers to the legitimate users.

A mobile device transmission is said to be secure if $\xi(\varepsilon) \geq \upsilon_s$, where υ_s denotes the minimum required secrecy probability.

Lemma 10. *An upper bound for the secrecy rate threshold for secure communication in the high SINR regime is given by:*

$$\varepsilon \leq \frac{\alpha}{2} \log_2 \left(\frac{-\lambda_E}{\mathrm{E}\left[P_E^{\frac{2}{\alpha}}\right]^{-1} \tilde{\Omega} \log \upsilon_s} \right). \tag{6.12}$$

The secure transmission region, $\mathscr{A}_{\mathrm{s}}(\mu_{\mathrm{s}}, \upsilon_{\mathrm{s}}) \subset \mathbb{R}^2$, around a typical mobile transmitter is random and defined as the range within which eavesdroppers cannot intercept the communication with high probability. In other words, $\mathscr{A}_{\mathrm{s}}(\mu_{\mathrm{s}}, \upsilon_{\mathrm{s}})$ is the region where the set of all eavesdroppers are located outside a closed ball $\mathscr{B}\left(o, 2^{\varepsilon/\alpha}\|x_o\|\right)$ centered around the typical mobile transmitter located at $\|x_o\|$ with radius $2^{\varepsilon/\alpha}\|x_o\|$ [306]. Therefore we can use the upper bound on ε defined in Eq.(6.12) to define $\mathscr{A}_{\mathrm{s}}(\mu_{\mathrm{s}}, \upsilon_{\mathrm{s}})$ as:

$$\mathscr{A}_s(\mu_{\mathrm{s}}, \upsilon_{\mathrm{s}}) = \left\{ x \in \mathbf{R}^2 : \|e - x_o\| > \mu_{\mathrm{s}} = 2^{\varepsilon/\alpha}\|x_o\| \right\}. \tag{6.13}$$

In case of transmitting to the furthest neighbor:

$$\mu_{\mathrm{s}} \leq \int_0^{d_{\max}} 2^{\varepsilon/\alpha} r f_{L_{\mathrm{f}}}(r) dr = 2^{\varepsilon/\alpha} \frac{d_{\max} e^{d_{\max}^2 \phi/2} - c}{e^{d_{\max}^2 \phi/2} - 1}, \tag{6.14}$$

where $\varepsilon = (\alpha/2) \log_2 \left(-\lambda_{\mathrm{E}} / \left(\mathrm{E}\left[P_{\mathrm{E}}^{\frac{2}{\alpha}}\right]^{-1} \tilde{\Omega} \log \upsilon_s \right) \right)$; $c = \sqrt{\pi/(2\phi)}\mathrm{erfi}\left(\frac{d_{\max}}{2}\sqrt{2\phi}\right)$; and $\mathrm{erfi}(x) = 2/\sqrt{\pi}\int_0^x e^{t^2} dt$ is the imaginary error function.

In case of transmitting to the nearest neighbor:

$$\mu_{\rm s} \leq \int_0^{\infty} 2^{\varepsilon/\alpha} r f_{L_{\rm c}}(r) dr = 2^{\varepsilon/\alpha} \sqrt{\frac{\pi}{2\lambda_{\rm MANET}\phi}}, \tag{6.15}$$

where $\varepsilon = (\alpha/2)\log_2\left(-\lambda_{\rm E}/\left(\mathrm{E}\left[P_{\rm E}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}\log \upsilon_s\right)\right)$.

Thus, the transmission region $\mathscr{A}_{\rm r}(\mu_{\rm r}, \nu, \upsilon_{\rm s}) \subset \mathbb{R}^2$ around a typical mobile transmitter that satisfies a secrecy rate $\xi(\varepsilon) \geq \upsilon_{\rm s}$ and a target outage probability ν is defined as:

$$\mathscr{A}_{\rm r}(\mu_{\rm r}, \nu, \upsilon_{\rm s}) = \left\{x \in \mathbf{R}^2 : \|x\| < \mu_{\rm r}, \mu_{\rm r} = \min\{\mu_{\rm s}, \mu_{\rm c}\}\right\}. \tag{6.16}$$

6.3.3 No Information on Eavesdroppers

In this scenario, the malicious users are not known to the legitimate users. Thus, we consider the worst-case scenario that all users are malicious [307, 308] and form a homogeneous PPP $\Phi_{\rm I}$ of intensity $\lambda_{\rm I} = \lambda_{\rm I}^{\rm CN} + \lambda_{\rm I}^{\rm a,MBAN} + \lambda_{\rm I}^{\rm MANET} + \lambda_{\rm I}^{\rm E}$, since the superposition of independent PPP is also a PPP [309]. We are interested in a state $\mathscr{S}$ where all interferers are located outside region $\mathscr{B}(o, R_{\rm c})$. A transmission region is said to be secure if the probability of the interference power received by the mobile user falling below ε is greater than υ_s. Thus, the interference samples received by the typical mobile device outside region $\mathscr{B}$ can be expressed as

$$\mathscr{S}: \qquad y[n] = \sum_{i \in \phi_{\rm I} \cap \mathscr{B}^c} s_i[n] + z[n], \tag{6.17}$$

where $n = 0, 1, ..., N-1$ is the sample index with N being the total number of samples; $s_i[n] = \left(P_{{\rm I},o} h_{io} l(i,o)\right)[n]$ is the nth sample of the received signal from interferer i by a typical mobile user; $z[n]$ is the Gaussian noise ($z[n] \sim \mathscr{N}(0, \sigma_n^2)$); $\phi_{\rm I}$ is a realization of $\Phi_{\rm I}$ denoting the set of interferers' locations; and $\mathscr{B}^c$ is the complementary set of $\mathscr{B}$. The average received interference power can be expressed as $\zeta = 1/N \sum_{n=0}^{N-1} y[n]$. When N is large, by central limit theorem, the distribution of ζ

approaches Gaussian distribution. Thus, we can characterize the mean and variance of ζ as [219]:

$$\begin{aligned} \mathrm{E}(\zeta) &= \sum_{i\in\tilde{\phi}_{\mathrm{I}},|\mathscr{B}|=0} P_{\mathrm{I},i} h_{io} l(i,o) = I_{\mathrm{I}}, \\ Var(\zeta) &= \frac{1}{N^2}\left(I_{\mathrm{I}} + \sigma_n^2\right), \end{aligned} \tag{6.18}$$

where $|\mathscr{B}|$ denotes the number of interferers inside region $\mathscr{B}$. As can be seen in Eq. (6.18), the random variable I_{I} depends on the spatial distribution of interferers. Because the secrecy of the link depends heavily on I_{I}, we can express the average probability that a mobile link is secure as:

$$\xi(\varepsilon) = \frac{\lambda_{\mathrm{MANET}}}{\lambda_{\mathrm{tot}}} \int_0^{\infty} f_{I_{\mathrm{I}}}(x)\, \mathscr{P}\left(\zeta < \varepsilon | I_{\mathrm{I}}, \mathscr{S}\right) dx, \tag{6.19}$$

where $\lambda_{\mathrm{tot}} = \lambda_{\mathrm{MANET}} + \lambda_{\mathrm{MBAN}} + \lambda_{\mathrm{CN}} + \lambda_{\mathrm{E}}$; $f_{I_{\mathrm{I}}}(x)$ is the PDF of I_{I}; and $\mathscr{P}\left(\zeta < \varepsilon | I_{\mathrm{I}}\right) = 1 - Q\left(\frac{N(\varepsilon - x)}{\sqrt{x+\sigma_n^2}}\right)$, where Q-function is the tail probability of the standard normal distribution. Next, we obtain an expression for $f_{I_{\mathrm{I}}}(x)$ in order to characterize $\xi(\varepsilon)$.

Lemma 11. *An expression of the Laplace transform of I_I can be obtained as:*

$$\begin{aligned} \mathscr{L}_{I_I}(s) &= \mathrm{E}[e^{-sI_I}] \\ &= \exp\left(-2\pi\lambda_I \int_{R_c}^{\infty} \left(1 - \mathrm{E}_{P_I}\left[\frac{1}{1+sP_I r^{-\alpha}}\right]\right) rdr\right) \\ &= \exp\left(-\frac{2\pi\lambda_I s}{(\alpha-2)R_c^{\alpha-2}} \mathrm{E}\left[{}_2F_1\left(1, 1-\frac{2}{\alpha}; 2-\frac{2}{\alpha}; -\frac{sP_I}{R_c^{\alpha}}\right) P_I\right]\right). \end{aligned} \tag{6.20}$$

For the special case of $\alpha = 4$, $\mathscr{L}_{I_{\mathrm{I}}}(s)$ becomes:

$$\mathscr{L}_{I_{\mathrm{I}}}(s) = \exp\left(-R_{\mathrm{c}}^{-2}\sqrt{s}\mathrm{E}\left[\sqrt{P_{\mathrm{I}}}\arctan\left(\frac{\sqrt{sP_{\mathrm{I}}}}{R_{\mathrm{c}}^2}\right)\right]\right). \tag{6.21}$$

The PDF of I_{I} can be accurately approximated by a log normal distribution [310, 311] as:

$$f_{I_{\mathrm{I}}}(x) \approx \frac{1}{x\vartheta\sqrt{2\pi}} \exp\left(\frac{-\log(x/m)^2}{2\vartheta^2}\right), \tag{6.22}$$

where $\vartheta^2 = \log\left(\kappa_2/\kappa_1^2 + 1\right)$; $m = \kappa_1/\exp(\vartheta^2/2)$; $\kappa_1 = \mathrm{E}[P_\mathrm{I}]/R_\mathrm{c}^4$; and $\kappa_2 = 2\mathrm{E}[P_\mathrm{I}^2]/(3R_\mathrm{c}^8)$.

Theorem 16. *In interference-limited networks, the average probability that a mobile link is secure can be expressed as:*

$$\begin{aligned}\xi(\varepsilon) &= \frac{\lambda_{MANET}}{\lambda_{tot}} \int_0^\infty Q\left(\frac{-N(\varepsilon - x)}{\sqrt{x+\sigma_n^2}}\right) f_{I_I}(x)dx \\ &\overset{(a)}{\approx} \frac{\lambda_{MANET}}{\lambda_{tot}} \left(1 - \int_\varepsilon^\infty \frac{\exp\left(-\frac{\log(x/m)^2}{2\vartheta^2}\right)}{x\vartheta\sqrt{2\pi}}\right) \\ &= \frac{\lambda_{MANET}}{\lambda_{tot}} \left(1 - Q\left(\frac{\log\varepsilon - \log m}{\vartheta}\right)\right),\end{aligned} \tag{6.23}$$

where (a) comes from the fact that the Q-function can be approximated by a step function in interference-limited regime [312].

Corollary 3. *An upper bound for the secrecy rate threshold for secure communication in interference-limited regime is given by:*

$$\xi(\varepsilon) \geq \upsilon_s \Rightarrow \varepsilon < m\exp\left(\vartheta Q^{-1}\left(1 - \upsilon_s e^{-\pi\lambda_{MANET}R_c^2}\right)\right). \tag{6.24}$$

Therefore, in case of transmitting to the furthest neighbor,

$$\mu_\mathrm{s} < 2^{\frac{m}{\alpha}\exp\left(\vartheta Q^{-1}\left(1-\upsilon_s e^{-\pi\lambda_\mathrm{MANET}R_\mathrm{c}^2}\right)\right)} \frac{d_\mathrm{max} e^{d_\mathrm{max}^2\phi/2} - c}{e^{d_\mathrm{max}^2\phi/2} - 1}. \tag{6.25}$$

In case of transmitting to the nearest neighbor:

$$\mu_\mathrm{s} < 2^{\frac{m}{\alpha}\exp\left(\vartheta Q^{-1}\left(1-\upsilon_s e^{-\pi\lambda_\mathrm{MANET}R_\mathrm{c}^2}\right)\right)} \sqrt{\frac{\pi}{2\lambda_\mathrm{MANET}\phi}}, \tag{6.26}$$

Thus, the transmission region $\mathscr{A}_\mathrm{r}(\mu_\mathrm{r}, \nu, \upsilon_\mathrm{s}) \subset \mathbb{R}^2$ around a typical mobile transmitter that sat-

isfies a secrecy rate $\xi(\varepsilon) \geq \upsilon_{\rm s}$ and a target outage probability ν is defined as:

$$\mathscr{A}_{\rm r}(\mu_{\rm r}, \nu, \upsilon_{\rm s}) = \left\{x \in \mathbf{R}^2 : \|x\| < \mu_{\rm r}, \mu_{\rm r} = \min\{\mu_{\rm c}, \mu_{\rm s}\}\right\}. \tag{6.27}$$

6.3.4 End-to-End Delay Analysis

In this section we analyze the mean end-to-end delay defined as the average number of time slots required for the packet to reach the destination. We use the random-sequential totally asymmetric simple exclusion process (random-sequential TASEP) as defined in [298, 313], which describes system dynamics with interacting particles (or packets). Considering $\bar{L}+1$ sites (or nodes) in the system, then a single site is uniformly randomly picked for transmission with probability $1/(\bar{L}+1)$. The picked site is denoted as site 0 (source node) which performs hopping with probability $p_{\rm s}$ through $\bar{L}$ sites to reach the destination site. The configuration site $\tau_i[t]$ defines whether a site is occupied at time t, i.e. has a packet in its buffer ($\tau_i[t] = 1$) or empty ($\tau_i[t] = 0$). The probability that a node is occupied is equal to the average number of packets at node i's buffer. The occupancy of source and destination nodes are given in [[298], Eq. 8]:

$$\mathrm{E}[\tau_1] = \frac{3\bar{L}}{2\,(2\bar{L}+1)} \quad \text{and} \quad \mathrm{E}[\tau_{\bar{L}}] = \frac{\bar{L}+2}{2\,(2\bar{L}+1)}, \tag{6.28}$$

with the average number of occupied nodes: $\sum_{i=0}^{\bar{L}} \mathrm{E}[\tau_i] = 1 + \bar{L}/2$. Next, we find the average number of hops in the system.

The area of transmission region of a typical mobile transmitter is defined as [314]:

$$|\mathscr{A}_{\rm r}(\mu_r, \nu, \upsilon_s)| = \int_{\mathbb{R}^2} \Pi_{y \in \Phi_{\rm MANET}} \mathbb{1}(\|x\| < \mu_{\rm r}) dx. \tag{6.29}$$

The average transmission area can be expressed as

$$\begin{aligned}
\mathrm{E}[|\mathscr{A}_{\mathrm{r}}(\mu_r,\nu,\upsilon_s)|] &= \mathrm{E}\mathrm{E}^{o}_{\Phi_{\mathrm{MANET}}}[|\mathscr{A}_{\mathrm{r}}\mu_{\mathrm{r}},\nu,\upsilon_s)|] \\
&= \mathrm{E}\mathrm{E}_{\Phi_{\mathrm{MANET}}}[|\mathscr{A}_{\mathrm{r}}(\mu_{\mathrm{r}},\nu,\upsilon_s)|] \\
&= \int_{\mathbb{R}^2} \mathbf{E}_{\Phi_{\mathrm{MANET}}}\Pi_{y\in\Phi_{\mathrm{MANET}}}\mathbb{1}(\|x\|<\mu_{\mathrm{r}})dx \\
&= \int_{\mathbb{R}^2} e^{-\lambda_{\mathrm{MANET}}\mathbb{1}(\|x\|<\mu_{\mathrm{r}})}dx = e^{-\lambda_{\mathrm{MANET}}\pi\mu_{\mathrm{r}}^2}.
\end{aligned} \tag{6.30}$$

We define the number of all relay users located in the transmission region, $\mathscr{A}_{\mathrm{r}}(\mu_r,\nu,\upsilon_s)$, of the typical user o as $N_{\mathrm{r}} = |\forall\{j\in\Phi_{\mathrm{MANET}}\setminus o\}|\cap\mathscr{A}_{\mathrm{r}}(\mu_r,\nu,\upsilon_s)$[4]. N_{r} is a Poisson random variable with mean $\lambda_{\mathrm{MANET}}\mathrm{E}[|\mathscr{A}_{\mathrm{r}}(\mu_r,\nu,\upsilon_s)|]$. It should be noted that N_{r} is not a function of relay users' locations j.

The average number of hops in the system becomes: $\bar{L} = \lambda_{\mathrm{MANET}}/N_{\mathrm{r}}$. At steady state (as $t\to\infty$), the spatial throughput at steady-state becomes [298]: $T(\bar{L}) = p_{\mathrm{s}}/(2\bar{L}+1)$. By Little's theorem, the average end-to-end delay[5] is expressed as [298]

$$D(\bar{L}) = \frac{\sum_{i=0}^{\bar{L}}\mathrm{E}[\tau_i]}{T} = \frac{2\bar{L}^2+5\bar{L}+2}{2p_{\mathrm{s}}}. \tag{6.31}$$

In case of transmitting to the furthest neighbor:

$$D(\bar{L}) = \frac{\Delta_1\left(2e^{2\lambda_{\mathrm{MANET}}\pi\mu_{\mathrm{r}}^2}+5e^{\lambda_{\mathrm{MANET}}\pi\mu_{\mathrm{r}}^2}+2\right)}{1-e^{\mu_{\mathrm{c}}^2\left(\phi/2-\pi\theta^{\frac{2}{\bar{\alpha}}}\mathrm{E}\left[P_{\mathrm{MANET}}^{\frac{2}{\bar{\alpha}}}\right]^{-1}\tilde{\Omega}\right)}}, \tag{6.32}$$

$$\Delta_1 = \left(\pi\theta^{\frac{2}{\bar{\alpha}}}\mathrm{E}\left[P_{\mathrm{MANET}}^{\frac{2}{\bar{\alpha}}}\right]^{-1}\tilde{\Omega}-\phi/2\right)\left(e^{d_{\max}^2\phi/2}-1\right)\phi^{-1}.$$

[4] $|.|$ denotes the set cardinality.

[5] Queuing delay is neglected since we assume that source nodes always have packets to transmit.

In case of transmitting to the nearest neighbor:

$$D(\bar{L}) = \frac{\Delta_2 \left(2e^{2\lambda_{\text{MANET}}\pi\mu_{\text{r}}^2} + 5e^{\lambda_{\text{MANET}}\pi\mu_{\text{r}}^2} + 2\right)}{1 - e^{-\mu_{\text{c}}^2\left(\pi\theta^{\frac{2}{\alpha}}\text{E}\left[P_{\text{MANET}}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega} + \lambda_{\text{MANET}}\phi/2\right)}}, \tag{6.33}$$

$$\Delta_2 = \left(\pi\theta^{\frac{2}{\alpha}}\text{E}\left[P_{\text{MANET}}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega} + \lambda_{\text{MANET}}\phi/2\right)(\lambda_{\text{MANET}}\phi)^{-1}.$$

Let D_{Th} denotes the maximum allowable delay after which the packet needs to be discarded.

In case of transmitting to the furthest neighbor:

$$\begin{aligned} &D(\bar{L}) \leq D_{\text{Th}} \\ &\Rightarrow \mu_{\text{r}} \leq \sqrt{\frac{D_{\text{Th}}}{9\pi\lambda_{\text{MANET}}\rho_1} - \frac{1}{\pi\lambda_{\text{MANET}}}} \triangleq \mu_{\text{d}}, \end{aligned} \tag{6.34}$$

$$\rho_1 = \Delta_1 \Big/ \left(1 - \exp\left(\mu_{\text{c}}^2\left(\phi/2 - \pi\theta^{\frac{2}{\alpha}}\text{E}\left[P_{\text{MANET}}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}\right)\right)\right).$$

In case of transmitting to the nearest neighbor:

$$\mu_{\text{r}} \leq \sqrt{\frac{D_{\text{Th}}}{9\pi\lambda_{\text{MANET}}\rho_2} - \frac{1}{\pi\lambda_{\text{MANET}}}} \triangleq \mu_{\text{d}}, \tag{6.35}$$

where $\rho_2 = \Delta_2 \Big/ \left(1 - e^{-\mu_{\text{c}}^2\left(\pi\theta^{\frac{2}{\alpha}}\text{E}\left[P_{\text{MANET}}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega} + \lambda_{\text{MANET}}\phi/2\right)}\right)$.

The transmission region $\mathscr{A}_{\text{r}}(\mu_{\text{r}}, \nu, \upsilon_{\text{s}}, D_{\text{Th}})$ that satisfies a secrecy rate $\xi(\varepsilon) \geq \upsilon_s$, a target outage probability ν and a target end-to-end delay threshold D_{Th} is defined as

$$\mathscr{A}_{\text{r}}(\mu_{\text{r}}, \nu, \upsilon_{\text{s}}, D_{\text{Th}}) = \left\{x \in \mathbb{R}^2 : \|x\| < \mu_{\text{r}}, \mu_{\text{r}} = \min\{\mu_{\text{s}}, \mu_{\text{c}}, \mu_{\text{d}}\}\right\}. \tag{6.36}$$

6.4 Numerical Results and Analysis

In this section, we present numerical results to study the proposed security scheme for mobile computing network tier. Unless otherwise stated, we set the following system parameters: $N_{\mathrm{m}} = 1$ [300], $\alpha = 4$, $\lambda_{\mathrm{CN}} = \lambda_{\mathrm{MBAN}} = \lambda_{\mathrm{MANET}} = 10^{-1}$ m^{-2}; $\upsilon_s = 0.5$; $\delta = 10^{-5}$ dBm [295]; $\theta = 20$ dB (high SINR conditions) [306]; $\nu = 0.5$; $\phi = \pi/2$ [298]; $N = 5000$; and $d_{\max} = 3$ m.

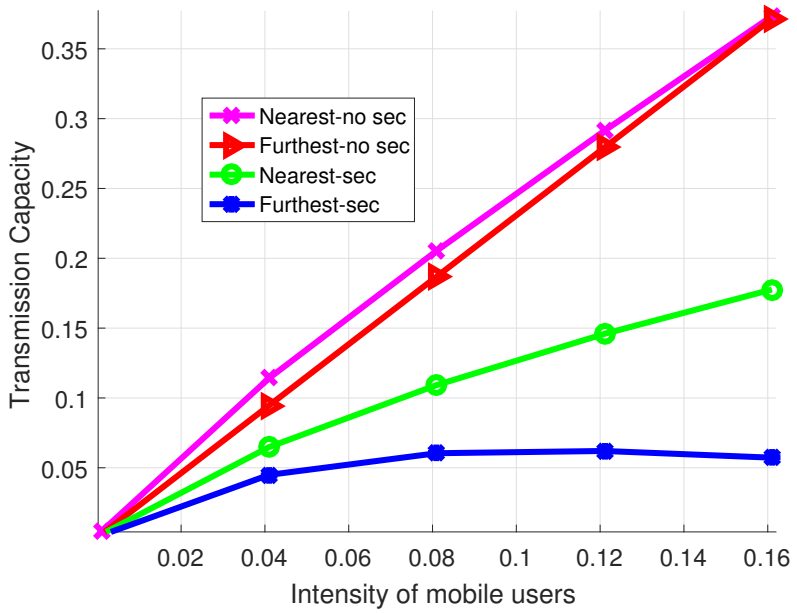

Figure 6.3: The average transmission capacity versus the intensity of mobile users under full information on eavesdroppers ($\lambda_{\mathrm{E}} = 10^{-2}$).

Fig. 6.3 depicts the average transmission capacity, i.e., the density of successful transmissions at a rate $\log(1+\theta)$, expressed as $\Upsilon = \lambda_{\mathrm{MANET}} \log(1+\theta) p_{\mathrm{s}}$ [279]. Under the proposed security scheme, the transmitter restricts its transmission power to the secure transmission region $\mathscr{A}_{\mathrm{s}}$, leading to a higher secrecy probability but at the expense of fewer number of transmissions. However, when secure transmission is not employed, the transmitter is able to extend its range of communications to a larger number of users, but at the expense of compromising its protection from eavesdroppers. Furthermore, transmitting to the nearest neighbor achieves higher transmission capacity compared to when transmitting to the furthest neighbor, due to increasing the probability of successful transmissions, as will be explained in Fig. 6.7.

Fig. 6.4 shows the average secrecy probability $\xi(\varepsilon)$ versus the intensity of eavesdroppers λ_{E}. First, the average secrecy probability decreases as λ_{E} increases mainly due to reducing the distances between legitimate users and eavesdroppers. Second, when the mobile user has full information on the eavesdroppers in the network, it can achieve much higher secrecy probability than that of the scenario without information on malicious users, since the latter treats all interferers as eavesdroppers (worst-case scenario). This is especially true for a smaller population of eavesdroppers. Third, when transmitting to the nearest neighbor, the secrecy probability is higher than when transmitting to the furthest neighbor.

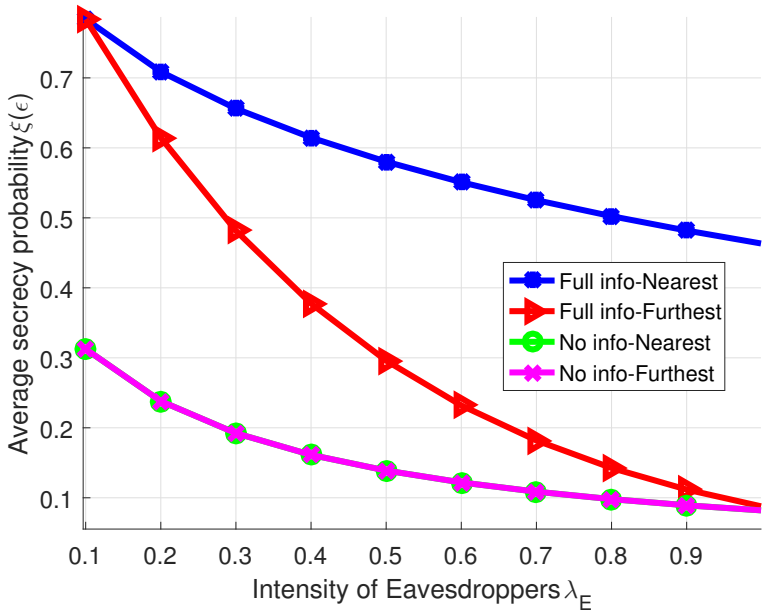

Figure 6.4: The average secrecy probability $\xi(\varepsilon)$ versus the intensity of eavesdroppers ($R_{\mathrm{c}} = 10$ m and $\varepsilon = 0.5$).

Fig. 6.5 shows the secure transmission distance μ_{s} versus the intensity of mobile users.Transmitting to the nearest neighbor achieves higher μ_{s} than when transmitting to the furthest neighbor, due to larger distances from the interferers to the mobile user. Furthermore, it can be seen that the full information on eavesdroppers scenario achieves much higher secure transmission distance.

Fig. 6.6 plots the transmission distance $\mu_{\mathrm{r}} = \min\{\mu_{\mathrm{s}}, \mu_{\mathrm{c}}\}$ for the no information on eavesdroppers scenario versus the intensity of mobile users for different values of R_{c}. Transmitting to the nearest neighbor achieves the highest transmission distance that guarantees a target outage proba-

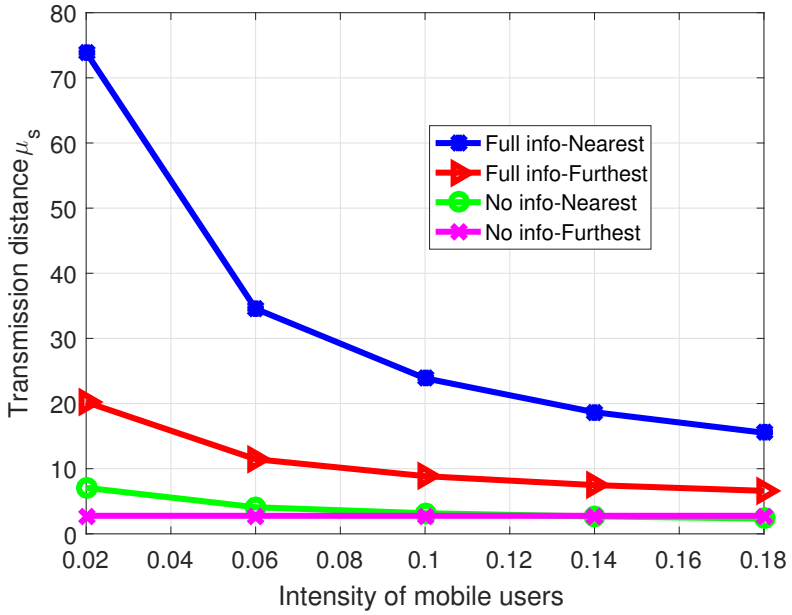

Figure 6.5: The secure transmission distance μ_s versus the intensity of mobile users ($R_c = 10$ m).

bility ν and a secrecy probability υ_s. As R_c increases, the interference inside region $\mathscr{B}$ becomes higher, leading to a decrease in the secure transmission region. Note that for all values of R_c, transmitting to the furthest neighbor achieves the lowest μ_r since it is constrained with the small secure transmission distance μ_s.

Fig. 6.7 depicts the mean end-to-end delay versus λ_{MANET}. When information on eavesdroppers is available, transmitting to the nearest neighbor achieves the lowest delay due to higher successful transmission probability p_s. Furthermore, transmitting to the nearest neighbor without information on eavesdroppers achieves lower delay than the case of transmitting to the furthest neighbor. It is interesting to see that beyond $\lambda_{\text{MANET}} = 0.14$, the no information-nearest neighbor case becomes worse than the no information-furthest case since the latter is not in function of mobile users' intensity, so it remains constant throughout.

To study the achievable trade-off between the delay and the secrecy, we plot Fig. 6.8, which shows an almost linear behavior for the ratio $D(\bar{L})/\xi(\varepsilon)$ in terms of λ_E for all the cases except for the full information-furthest case which increases exponentially. As can be seen, transmitting to the nearest neighbor with full information on eavesdroppers achieves the best trade-off between

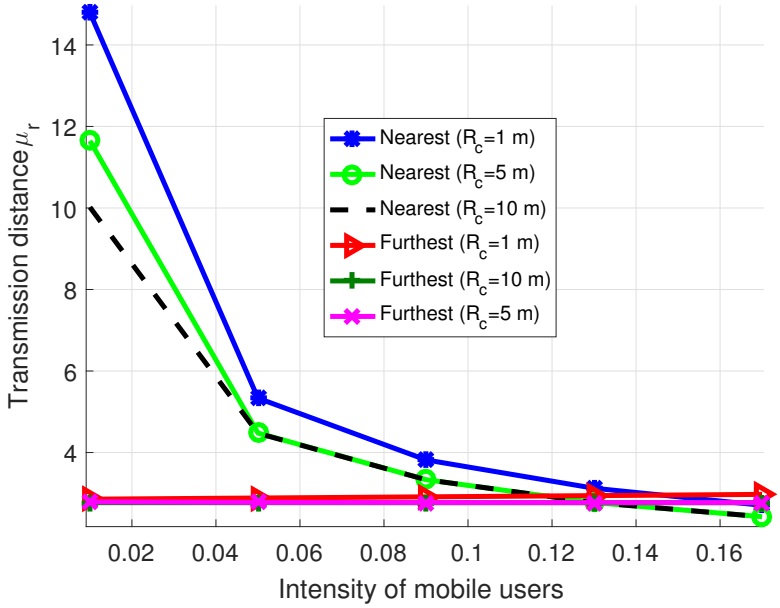

Figure 6.6: The transmission distance $\mu_r = \min\{\mu_s, \mu_c\}$ versus the intensity of mobile users ($\lambda_E = 10^{-2}$).

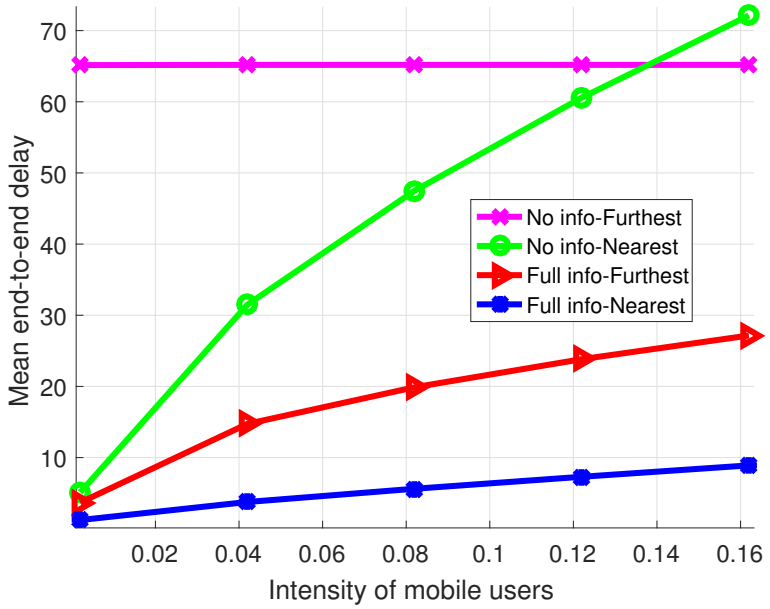

Figure 6.7: Mean end-to-end delay versus the intensity of mobile users that guarantees a secrecy probability υ_s (source node is assumed to be 25 m away from the destination node).

delay and secrecy, followed by the case of transmitting to the furthest neighbor. When the mobile user does not have information on users' behaviors, it is always better to transmit to the nearest neighbor rather than to the furthest one.

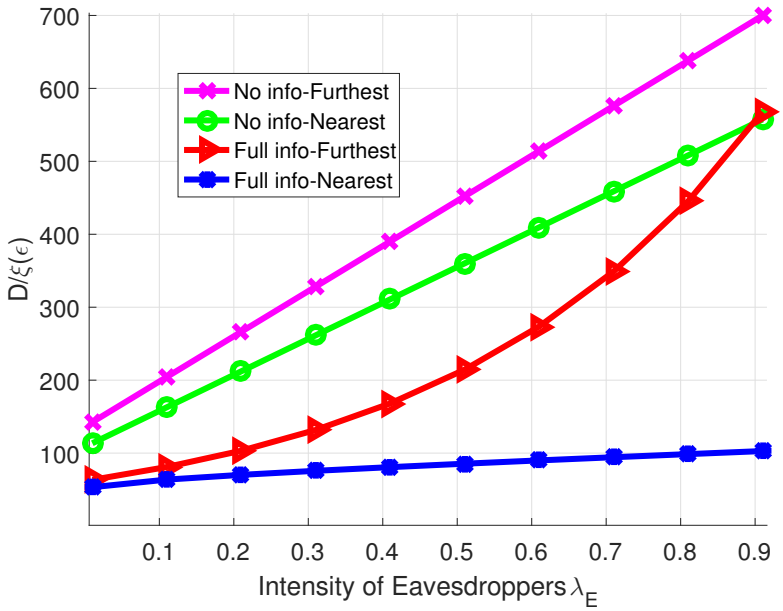

Figure 6.8: The plot of $D(\bar{L})/\xi(\varepsilon)$ versus the intensity of eavesdroppers ($R_c = 10$ m; $\varepsilon = 0.5$; and source node is assumed to be 25 m away from the destination node).

Finally, Fig. 6.9 shows the transmission distance $\mu_r = \min\{\mu_s, \mu_c, \mu_d\}$ versus λ_E for different values of D_{Th}. As the delay threshold deadline is relaxed, so is the transmission distance. Beyond $D_{Th} = 50$ seconds, we do not see much changes to μ_r since it becomes constrained by the minimum among μ_c and μ_s excluding μ_d. In other words, we see similar performance as in Fig. 6.6.

Discussions and Insights

By defining a secure ranging distance around a typical transmitter using stochastic geometry tools, we showed that the transmitter was able to communicate with its neighbors with high average secrecy probability, without the need for complex calculations to estimate the legitimate neighbors distances like in [271, 272], and without the need for sophisticated secure protocols such as RF fingerprinting [274] or forbidden structures identification in connectivity graphs [315]. By learning about users' behaviors and trustworthiness, the transmitter was able to extend its secure communication range, while achieving a low mean end-to-end delay, a critical requirement for sensitive

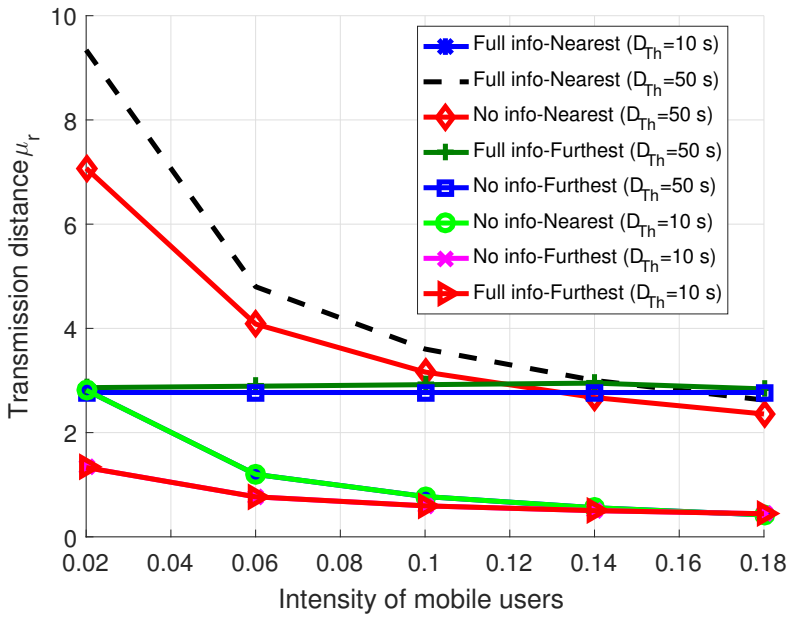

Figure 6.9: The transmission distance $\mu_r = \min\{\mu_s, \mu_c, \mu_d\}$ versus the intensity of mobile users for different values of D_{Th} ($R_c = 10m$ and $\lambda_E = 10^{-2}$).

medical data. Furthermore, we showed that the cost of securely communicating with neighboring devices is a decreased transmission capacity due to limiting the communication range between devices.

6.5 Conclusions

In this chapter, we have proposed a physical layer security scheme for mobile computing tier in m-Health CPS using tools from stochastic geometry. We have analytically derived expressions for the transmission region around a typical mobile user that satisfies a secrecy probability, a target outage probability and a delay threshold constraints. Furthermore, we have provided analysis on the average end-to-end delay across a typical link. We have compared these performance metrics in two different scenarios: when information on users' behaviors is available and when it is unavailable. In addition, we considered two cases: i) when mobile user transmits to the nearest neighbor, and ii) when it transmits to the furthest neighbor. Numerical results have shown that being equipped with information on eavesdroppers can benefit the system performance in terms of secrecy and latency.

On the other hand, when that information cannot be obtained, it is always best to transmit to the nearest neighbor.

Chapter 7

List of Related Publications

7.1 Conference papers

- **Atat, R.**, Liu, L. and Yi, Y., "Privacy Protection Scheme for eHealth Systems: A Stochastic Geometry Approach", 2016 IEEE Global Communications Conference (GLOBECOM'16), Washington, DC USA, Dec. 2016.

- **Atat, R.**, Liu, L., Ashdown, J., Medley, M., Matyjas, J., and Yi, Y., "Improving Spectral Efficiency of D2D Cellular Networks Through RF Energy Harvesting", 2016 IEEE Global Communications Conference (GLOBECOM'16), Washington, DC USA, Dec. 2016. **(BEST PAPER AWARD)**

- **Atat, R.** and Liu, L., Ashdown, J., Medley, M., and Matyjas, J. "On the Performance of Relay-Assisted D2D Networks under Spatially Correlated Interference", 2016 IEEE Global Communications Conference (GLOBECOM'16), Washington, DC USA, Dec. 2016.

- **Atat, R.**, Chen, H. and Liu, L., Ashdown, J., Medley, M., and Matyjas, J., "Fundamentals of Spatial RF Energy Harvesting for D2D Cellular Networks", 2016 IEEE Global Communications Conference (GLOBECOM'16), Washington, DC USA, Dec. 2016.

- **Atat, R.** and Liu,L., "On the Achievable Transmission Capacity of Secrecy-Based D2D

Cellular Networks", 2016 IEEE Global Communications Conference (GLOBECOM'16), Washington, DC USA, Dec. 2016.

- Wu,S., **Atat, R.**, Mastronarde,N., and Liu,L. "Coverage Analysis of D2D Relay-Assisted Millimeter-Wave Cellular Networks", 2017 IEEE Wireless Communications and Networking Conference WCNC, San Fransisco, CA USA, March 2017.

- Chen, H., Shafin, R., **Atat, R.**, Yi, Y., and Liu, L., "Performance Analysis on Nano-Networks: A Stochastic Geometry Approach", Proceedings of the 3rd ACM International Conference on Nanoscale Computing and Communication, NANOCOM 2016, New York, NY, USA, September 28-30, 2016

7.2 Journals

- **Atat, R.**, Liu, L., Chen, H., Wu, J., Li, H., and Yi, Y. "Enabling Cyber-Physical Communication in 5G Cellular Networks: Challenges, Spatial Spectrum Sensing, and Cyber-Security', *IET Cyber-Physical Systems: Theory & Applications*.

- **Atat, R.**, Liu, L., Mastronarde, N. and Yi, Y. "Energy Harvesting-Based D2D-Assisted Machine-Type Communications", *IEEE Transactions on Communications*, vol. 65 (3), March 2017.

- **Atat, R.**, Liu, L., Wu, J., Ashdown, J., and Yi, Y. "Green Massive Traffic Offloading for Cyber-Physical Systems over Heterogeneous Cellular Networks", *Mobile Networks and Applications Springer Journal*.

- **Atat, R.**, Liu, L., Ashdown, J., Medley, M., Matyjas, J., and Yi, Y. "A Physical Layer Security Scheme for Mobile Health Cyber-Physical Systems", *IEEE Transactions on Internet of Things* (under revision).

- **Atat, R.**, Liu, L., Wu, J., Li, G., Ye, C., Yi, Y. "Big Data Meet Cyber-Physical Systems: A Panoramic Survey", *IEEE Communications Surveys and Tutorials* (under revision).

- Hamedani, K., Liu, L., **Atat, R.**, Wu, J., Yi, Y. "Reservoir Computing Meets Smart Grids: Attack Detection using Delayed Feedback Networks", *IEEE Transactions on Industrial Informatics.* (under revision)

- Li, J.; Liu, L.; Zhao, C.; Hamedani, K.; **Atat, R.**; Yi, Y. "Enabling Sustainable Cyber Physical Security Systems Through Neuromorphic Computing", *IEEE Transactions on Sustainable Computing.* (under revision)

Chapter 8

Appendix

8.1 Proof of Lemma 1

For a tractable and accurate analysis, we consider the aggregated RF interference at D2D user as the sum of the interference I_0 coming from CUs outside $\mathscr{A}_h$ and the interference coming from inside $\mathscr{A}_h$. We assume a typical D2D user at the origin using Slivniyaks theorem. Let $\mathscr{A}_h^c$ be the complementary set of $\mathscr{A}_h$.

$$\begin{aligned}
\mathscr{L}_{I_{\mathrm{RF}}}(s) &= \mathrm{E}_{\Phi_C}\left[\exp\left(-s\sum_{\substack{x_i\in\tilde{\Phi}_C\cap\mathscr{A}_h\\ \tilde{\Phi}_C\cap\mathscr{A}_h\neq\emptyset}} P_C h_{x_i,0} l(x_i,0)\right)\right]\mathrm{E}_{\Phi_C}\left[\exp\left(-s\sum_{x_i\in\tilde{\Phi}_C\cap\mathscr{A}_h^c} P_C h_{x_i,0} l(x_i,0)\right)\right] \\
&\overset{(a)}{=} \frac{\sum_{k=1}^{\infty}\mathscr{P}(N(\mathscr{A}_h)=k)\mathrm{E}\left[\exp\left(-sP_C h_{x_i,0} l(x_i,0)\right)\right]^k}{1-e^{-\tilde{\lambda}_C\pi R_h^2}}\mathscr{L}_{I_0}(s) \\
&= \frac{e^{-\tilde{\lambda}_C\pi R_h^2}}{1-e^{-\tilde{\lambda}_C\pi R_h^2}}\mathscr{L}_{I_0}(s)\sum_{k=1}^{\infty}\frac{(\tilde{\lambda}_C\pi R_h^2)^k}{k!}\mathrm{E}\left[\frac{1}{1+sP_C l(x_i,0)}\right]^k \\
&= \mathscr{L}_{I_0}(s)\frac{\sum_{k=0}^{\infty}\frac{(\tilde{\lambda}_C\pi R_h^2)^k}{k!}\mathrm{E}\left[\frac{1}{1+sP_C l(x_i,0)}\right]^k - \mathscr{L}_{I_0}(s)e^{-\tilde{\lambda}_C\pi R_h^2}}{1-e^{-\tilde{\lambda}_C\pi R_h^2}} \\
&= \frac{\exp\left(-\frac{2\tilde{\lambda}_C\pi^2(s)^{2/\alpha}P_C^{2/\alpha}}{\alpha\sin(2\pi/\alpha)}\right) - \mathscr{L}_{I_0}(s)e^{-\tilde{\lambda}_C\pi R_h^2}}{1-e^{-\tilde{\lambda}_C\pi R_h^2}},
\end{aligned}$$

where (a) comes from the fact that transmitters are uniformly distributed and the number of transmitters follows a Poisson distribution. Note that the expression is conditioned on having at least one cellular transmitter inside $\mathscr{A}_h$.

Now, we need to find $\mathscr{L}_{I_0}(s)$. Let x_i be the location of CU and $y_i(x_i)$ be the location of corresponding serving BS. Let A be the event of $\|x_i\| \geq R_h$.

$$\begin{aligned}
\mathscr{L}_{I_0}(s) &= \mathrm{E}[e^{-sI_0}] \\
&= \mathrm{E}_{\Phi_C,\Phi_B,h}\left[\prod_{x_i\in\phi_C}\prod_{y_i\in\phi_B} e^{-sP_C h_{x_i,0} l(x_i,0)\mathbb{1}_{\{A\}}}\right] \\
&\overset{(a)}{=} \mathrm{E}_{\Phi_C,h}\left[\prod_{x_i\in\phi_C}\mathrm{E}_{\Phi_B}\prod_{\substack{y_i\in\phi_B \\ \|y_i-x_i\|\leq\|\phi_B-x_i\|}} e^{-sP_C h_{x_i,0} l(x_i,0)\mathbb{1}_{\{A\}}}\right] \\
&\overset{(b)}{=} \mathrm{E}_{\Phi_C,h}\left[\prod_{x_i\in\phi_C}\mathrm{E}_{\|x_i-y_i^*\|} e^{-sP_C h_{x_i,0} l(x_i,0)\mathbb{1}_{\{A\}}}\right] \\
&\overset{(c)}{\approx} \exp\left(-2\pi\lambda_B\int_{R_h}^{\infty}\left(1-\frac{1}{1+sP_C r^{-\alpha}}\right)rdr\right) \\
&= \exp\left(-\frac{2\pi\lambda_B P_C s}{(\alpha-2)R_h^{\alpha-2}}{}_2F_1\left(1,1-\frac{2}{\alpha};2-\frac{2}{\alpha};-\frac{sP_C}{R_h^{\alpha}}\right)\right),
\end{aligned}$$

where (a) comes from the independence of Φ_B and Φ_C and (b) comes from the fact that a CU would select the nearest BS. Note that the distances from CU to serving BSs are correlated; however this correlation is very weak and can be ignored [211], which justifies the approximation sign in (c).

8.2 Proof of Lemma 3

$$\begin{aligned}
F_{\mathrm{D_Z}}(d_z) &= \mathscr{P}(D_Z \leq d_z) \\
&= \mathscr{P}(D_X^2 + D_Y^2 - 2D_X D_Y\cos\phi \leq d_z^2) \\
&= \mathscr{P}(D_Y \leq \sqrt{d_z^2 - D_X^2 + 2D_X D_Y\cos\phi}).
\end{aligned}$$

Using Leibnitz Integration rule and having $f_{\mathrm{D}_X}(d_x), f_{\mathrm{D}_Y}(d_y), f_{\Phi}(\phi)$ independent, we get:

$$\begin{aligned} f_{\mathrm{D}_Z}(d_z) &= \frac{d}{d_{d_z}}\left[\int_{-\pi/2}^{\pi/2}\int_0^{R_\mathrm{r}}\int_0^{\sqrt{d_z^2-D_X^2+2D_XD_Y\cos\phi}} f_{\mathrm{D}_Y}(d_y)f_{\mathrm{D}_X}(d_x)f_{\Phi}(\phi)d(d_y)d(d_x)d\phi\right] \\ &= \int_{-\pi/2}^{\pi/2}\int_0^{R_\mathrm{r}} \frac{d_z}{\sqrt{2d_x^2d_y^2\cos\phi - d_x^2 + d_z^2}} f_{\mathrm{D}_Y}(\sqrt{2d_x^2d_y^2\cos\phi - d_x^2 + d_z^2}) f_{\mathrm{D}_X}(d_x) f_{\Phi}(\phi) d(d_x) d\phi \\ &= \int_{-\pi/2}^{\pi/2} f_{\Phi}(\phi) \int_0^{R_\mathrm{r}} \frac{4\pi\lambda_\mathrm{D} d_z}{\mu_\mathrm{m}^2\left(1-e^{-\pi\lambda_\mathrm{D}R_\mathrm{r}^2}\right)} d_x e^{-\pi\lambda_\mathrm{D}d_x^2} d(d_x) d\phi \\ &= \frac{2d_z}{\pi\mu_\mathrm{m}^2},\ 0 \le d_z \le \sqrt{\pi}\mu_\mathrm{m}. \end{aligned} \tag{8.1}$$

8.3 Proof of Theorem 6

The spectral efficiency of cellular users is defined by Proposition 3 in [1] as:

$$R_\mathrm{C} = \mathrm{E}^0_{\Phi_\mathrm{B},\Phi_\mathrm{C}}\left[\frac{1}{N}\right]\mathrm{E}\left[\log\left(1+\mathrm{SINR}\right)\right], \tag{8.2}$$

where N is a random variable representing the number of cellular transmitters in a cell. Considering a cell area S, and having Φ_B independent from Φ_C, we have:

$$\begin{aligned} &\mathrm{E}^0_{\Phi_\mathrm{B},\Phi_\mathrm{C}}\left[\frac{1}{N}\right] = \mathrm{E}_S\left[\mathrm{E}^0_{\Phi_\mathrm{C}}\left[\frac{1}{N(S)}|S\right]\right] \\ &= \mathrm{E}_S\left[\sum_{n=1}^{\infty}\frac{(S\lambda_\mathrm{C})^{n-1}e^{-S\lambda_\mathrm{C}}}{n(n-1)}\right] = \mathrm{E}_S\left[\frac{\left(1-e^{-S\lambda_\mathrm{C}}\right)}{S\lambda_\mathrm{C}}\right]. \end{aligned} \tag{8.3}$$

To obtain a closed-form expression for the PDF of S, we use a sufficiently accurate approximation as defined in [316]:

$$f_S(x) = \frac{343}{15}\sqrt{\frac{7}{2\pi}}(x\lambda_\mathrm{B})^{5/2}\exp\left(-\frac{7}{2}x\lambda_\mathrm{B}\right)\lambda_\mathrm{B}. \tag{8.4}$$

Substituting (8.4) in (8.3) gives;

$$\mathrm{E}^{0}_{\Phi_{\mathrm{B}},\Phi_{\mathrm{C}}}\left[\frac{1}{N}\right]=\frac{343\sqrt{7}\lambda_{\mathrm{B}}^{7/2}}{20\sqrt{2}\lambda_{\mathrm{C}}}\left[\left(\frac{7\lambda_{\mathrm{B}}}{2}\right)^{-\frac{5}{2}}-\left(\frac{7\lambda_{\mathrm{B}}}{2}+\lambda_{\mathrm{C}}\right)^{-\frac{5}{2}}\right].$$

To calculate $\mathrm{E}\left[\log\left(1+\mathrm{SINR}\right)\right]$, we use Theorem 3 in [317]:

$$\begin{aligned}\mathrm{E}\left[\log\left(1+\mathrm{SINR}\right)\right]=&\int_{r>0}2\pi r\lambda_{\mathrm{B}}e^{-\pi\lambda_{\mathrm{B}}r^{2}}\\&\int_{t>0}e^{-\sigma_{n}^{2}r^{\alpha}\left(2^{t}-1\right)}\mathscr{L}_{I_{\mathrm{BS}}}\left(r^{\alpha}\left(2^{t}-1\right)\right)dtdr,\end{aligned}\tag{8.5}$$

where $2\pi r\lambda_{\mathrm{B}}e^{-\pi\lambda_{\mathrm{B}}r^{2}}$ is the PDF of the transceiver distance. Substituting (8.5) in (8.2) analytically characterizes R_{C}.

8.4 Proof of Theorem 10

$$\begin{aligned}&\mathscr{P}\left(\gamma_{s,r}\geq\theta_{\mathrm{M}}\cap\gamma_{r,d}\geq\theta_{\mathrm{M}}|\Phi_{\mathrm{C}},\Phi_{\mathrm{D}},\Phi_{\mathrm{M}}\right)\\&=\mathscr{P}\left(P_{\mathrm{M}}h_{sr}l(s,r)\geq\theta_{\mathrm{M}}I_{r}^{t}\cap\hat{P}_{\mathrm{D}}h_{rd}l(r,d)\geq\theta_{\mathrm{M}}I_{d}^{t}|\Phi_{\mathrm{C}},\Phi_{\mathrm{D}},\Phi_{\mathrm{M}}\right)\\&=\mathrm{E}_{\{\Phi,I,l\}}\left[e^{-\frac{\theta_{\mathrm{M}}}{P_{\mathrm{M}}l(s,r)}I_{r}^{t}-\frac{\theta_{\mathrm{M}}}{\hat{P}_{\mathrm{D}}l(r,d)}I_{d}^{t}}\right]\\&=\mathrm{E}_{\{\Phi\}}\left[\prod_{x\in\Phi_{\mathrm{C}}\cap\mathscr{A}^{c}}\mathrm{E}_{l}\left[\frac{1}{1+\left(\frac{\theta_{\mathrm{M}}l(x,r)}{P_{\mathrm{M}}l(s,r)}\right)}\cdot\frac{1}{1+\left(\frac{\theta_{\mathrm{M}}l(x,d)}{\hat{P}_{\mathrm{D}}l(r,d)}\right)}\right]\right.\\&\cdot\prod_{x\in\tilde{\Phi}_{\mathrm{D}}}\mathrm{E}_{l}\left[\frac{1}{1+\left(\frac{\theta_{\mathrm{M}}l(x,r)}{P_{\mathrm{M}}l(s,r)}\right)}\cdot\frac{1}{1+\left(\frac{\theta_{\mathrm{M}}l(x,d)}{\hat{P}_{\mathrm{D}}l(r,d)}\right)}\right]\\&\left.\cdot\prod_{x\in\Phi_{\mathrm{M}}}\mathrm{E}_{l}\left[\frac{1}{1+\left(\frac{\theta_{\mathrm{M}}l(x,d)}{\hat{P}_{\mathrm{D}}l(r,d)}\right)}\right]\cdot\prod_{x\in\Phi_{\mathrm{C}}\cap\mathscr{A}}\mathrm{E}_{l}\left[\frac{1}{1+\left(\frac{\theta_{\mathrm{M}}l(x,r)}{P_{\mathrm{M}}l(s,r)}\right)}\right]\right].\end{aligned}$$

The PDF of the distance between relay and destination is given by Lemma 3. By transformation of random variables, we can obtain the PDF of $l(r,d)$ as $\left(2l^{-2/\alpha-1}\right)/\left(\alpha\pi\mu^{2}\right)$ for $1/\left(\sqrt{\pi}\mu\right)^{\alpha}\leq l\leq\infty$. A closed-form expression for $\mathrm{E}_{l(r,d)}\left[1/\left(1+\theta_{\mathrm{M}}l(x,d)/\left(\hat{P}_{\mathrm{D}}l(r,d)\right)\right)\right]$ cannot be obtained. Therefore, we use the following approximation obtained from numerical observations in [209]:

$\mathrm{E}\left[1/\left(1+Kr^{\alpha}\right)\right] \approx 1/\left(1+K^{2/\alpha}\mathrm{E}[r]^2\right)$. Then,

$$\mathrm{E}_l\left[\frac{1}{1+\frac{\theta_{\mathrm{M}} l(x,d)}{\hat{P}_{\mathrm{D}} l(r,d)}}\right] \approx \frac{1}{1+\left(\theta_{\mathrm{M}} l(x,d)\hat{P}_{\mathrm{D}}^{-1}\right)^{2/\alpha}\mathrm{E}[\|r-d\|]^2},$$

where $\mathrm{E}[\|r-d\|] = 2\sqrt{\pi}\mu/3$. Similarly, we can characterize

$$\mathrm{E}_{l(s,r)}\left[\frac{1}{1+\frac{\theta_{\mathrm{M}} l(x,r)}{P_{\mathrm{M}} l(s,r)}}\right] \approx \frac{1}{1+\left(\theta_{\mathrm{M}} l(x,r)P_{\mathrm{M}}^{-1}\right)^{2/\alpha}\mathrm{E}[\|s-r\|]^2},$$

where

$$\mathrm{E}[\|s-r\|] = \frac{2\pi\tilde{\lambda}_{\mathrm{D}}}{1-e^{-\pi\tilde{\lambda}_{\mathrm{D}}R_{\mathrm{r}}^2}}\left[\frac{\sqrt{\pi}\,\mathrm{erf}(\sqrt{\pi\tilde{\lambda}_{\mathrm{D}}}R_{\mathrm{r}})}{4\left(\pi\tilde{\lambda}_{\mathrm{D}}\right)^{3/2}} - \frac{R_{\mathrm{r}}e^{-\pi\tilde{\lambda}_{\mathrm{D}}R_{\mathrm{r}}^2}}{2\pi\tilde{\lambda}_{\mathrm{D}}}\right], \tag{8.6}$$

where $\mathrm{erf}(z) = (2/\sqrt{\pi})\int_0^z e^{-t^2}dt$ is the error function.

Using $\mathrm{E}\left[\prod_{x\in\Phi} v(x)\right] = \exp\left(-\lambda\int_{\mathbb{R}^2}[1-v(x)]dx\right)$ completes the proof.

8.5 Proof of Theorem 12

Since $h_k \sim \exp(1)$, then $\mathscr{P}(h_k \geq x) = e^{-x}$. We can write the following:

$$\begin{aligned}
\mathscr{P}(\gamma_k \geq \beta) &= \mathscr{P}\left(h_k \geq \beta r^{\alpha}P_k^{-1}(I_{\mathrm{tot},k}+\sigma^2)\right)\\
&= \mathrm{E}\left[\exp\left(-\beta r^{\alpha}P_k^{-1}(I_{\mathrm{tot},k}+\sigma^2)\right]\right.\\
&= \mathrm{E}_r\left[\exp\left(-\sigma^2\beta r^{\alpha}P_k^{-1}\right)\cdot\mathscr{L}_{I_{\mathrm{tot},k}}(\beta r^{\alpha}P_k^{-1})\right]
\end{aligned}$$

The Laplace transform of $\mathscr{L}_{I_{\mathrm{tot},k}}(\beta r^{\alpha}P_k^{-1})$ is given in Eq. (43) in [257] as:

$$\mathscr{L}_{I_{tot,k}}(\beta r^{\alpha}P_k^{-1}) = \exp\left(-\pi\tilde{\lambda}_k\bar{P}_{jk}^{2/\alpha}r^{2/\alpha}\frac{2\beta\bar{B}_{jk}^{2/\alpha-1}}{\alpha-2}{}_2F_1\left(1,1-\frac{2}{\alpha};2-\frac{2}{\alpha},-\frac{\beta}{\bar{B}_{jk}}\right)\right). \tag{8.7}$$

For interference-limited networks, we ignore the noise ($\sigma^2 = 0$). Then, according to [257]:

$$\begin{aligned}\mathscr{P}(\gamma_k \geq \beta) &= \prod_{j=0}^{K} \mathscr{L}_{I_{\text{tot},k}}(\beta r^{\alpha} P_k^{-1}) \\ &= \exp\left(-\pi \sum_{j=0}^{K} \tilde{\lambda}_k \bar{P}_{jk}^{2/\alpha} r^{2/\alpha} \frac{2\beta \bar{B}_{jk}^{2/\alpha-1}}{\alpha-2} {}_2F_1\left(1, 1-\frac{2}{\alpha}; 2-\frac{2}{\alpha}, -\frac{\beta}{\bar{B}_{jk}}\right)\right),\end{aligned}$$

which completes the proof.

8.6 Proof of Lemma 8

$$\begin{aligned}\mathscr{L}_{I_o}(s) &= \mathrm{E}_{\Phi_{\mathrm{I}}^{\text{MANET}}}\left[e^{-sI_o}\right] \\ &\overset{(a)}{=} \exp\Bigg(-\mathrm{E}_h\left[\int_0^{2\pi}\int_0^{\infty}\left(1-\mathrm{E}_{P_{\text{MANET}}}\left[e^{-sP_{\text{MANET}}hr^{-\alpha}}\right]\right)\lambda_{\mathrm{I}}^{\text{MANET}}\right. \\ &\cdot F_h\left(\frac{\delta r^{\alpha}}{\mathrm{E}[P_{\text{CN}}]}\right) F_h\left(\frac{\delta r^{\alpha}}{\mathrm{E}[P_{\text{MANET}}]}\right) F_h\left(\frac{\delta r^{\alpha}}{\mathrm{E}[P_{\text{MBAN}}]}\right) r dr d\theta\Bigg]\Bigg) \\ &\overset{(b)}{=} \exp\Bigg(-\frac{2\pi\lambda_{\mathrm{I}}^{\text{MANET}}\mathrm{E}[P_{\text{MANET}}^{\frac{2}{\alpha}}]}{\alpha\delta^{\frac{2}{\alpha}}}\int_0^{\infty}\frac{s\delta x^{\frac{2}{\alpha}-1}}{s\delta+x}\left(1-e^{-x}\right)dx \\ &\cdot \int_0^{\infty}\frac{s\delta y^{\frac{2}{\alpha}-1}}{s\delta+y}\left(1-e^{-y}\right)dy\int_0^{\infty}\frac{s\delta z^{\frac{2}{\alpha}-1}}{s\delta+z}\left(1-e^{-z}\right)dz\Bigg)\end{aligned}$$

where (a) comes from using the probability generating functional of the PPP; and (b) is obtained from [295] using $F_h(g) = 1 - e^{-g}$, and letting $x = \delta r^{\alpha}/\mathrm{E}[P_{\text{CN}}]$, $y = \delta r^{\alpha}/\mathrm{E}[P_{\text{MANET}}]$, and $z = \delta r^{\alpha}/\mathrm{E}[P_{\text{MBAN}}]$, which completes the proof.

8.7 Proof of Theorem 15

Let $\tilde{\Omega} = \omega/\operatorname{sinc}(2/\alpha)$. Since $h_{io} \sim \exp(1)$, then $\mathscr{P}(h_{io} \geq x) = e^{-x}$, then we can write the following:

$$\begin{aligned}
\mathscr{P}(\gamma_{i,o} \geq \theta) &= \mathscr{P}\left(\frac{h_{io} l(i,o) P_{\text{MANET,i}}}{I_o + \sigma^2} \geq \theta\right) \\
&= \mathrm{E}\left[\exp\left(-\theta l(i,o)^{-1} P_{\text{MANET},i}^{-1}\left(I_o + \sigma^2\right)\right)\right] \\
&\overset{(a)}{=} \mathrm{E}\left[\exp\left(-\pi\theta^{\frac{2}{\alpha}} r^2 \mathrm{E}\left[P_{\text{MANET}}^{\frac{2}{\alpha}}\right]^{-1} \tilde{\Omega}\right)\right] \\
&= \int_0^{\mu_c} \exp\left(-\pi\theta^{\frac{2}{\alpha}} r^2 \mathrm{E}\left[P_{\text{MANET}}^{\frac{2}{\alpha}}\right]^{-1} \tilde{\Omega}\right) \frac{r\phi e^{r^2\phi/2}}{e^{d_{\max}^2\phi/2} - 1} dr \\
&= \frac{\phi\left(1 - e^{\mu_c^2\left(\phi/2 - \pi\theta^{\frac{2}{\alpha}} \mathrm{E}\left[P_{\text{MANET}}^{\frac{2}{\alpha}}\right]^{-1} \tilde{\Omega}\right)}\right)}{2\left(\pi\theta^{\frac{2}{\alpha}} \mathrm{E}\left[P_{\text{MANET}}^{\frac{2}{\alpha}}\right]^{-1} \tilde{\Omega} - \phi/2\right)\left(e^{d_{\max}^2\phi/2} - 1\right)},
\end{aligned} \tag{8.8}$$

where in (a), we ignore the noise ($\sigma^2 = 0$). Similarly, we obtain the successful transmission probability when the typical mobile device is communicating with its nearest neighbor.

8.8 Proof of Corollary 2

From Appendix 8.7, we can write the following:

$$\mathscr{P}(\gamma_{i,o} \geq \theta) = \mathrm{E}_X\left[e^{-b_2 X^{\frac{2}{\alpha}}}\right], \tag{8.9}$$

where $X = r^\alpha$; and $b_2 = \pi\theta^{\frac{2}{\alpha}} \mathrm{E}\left[P_{\text{MANET}}^{\frac{2}{\alpha}}\right]^{-1} \tilde{\Omega}$.

We follow similar calculations to [318]:
Let $\chi(x) = e^{-b_2 x^{2/\alpha}}$, then $\chi'(x) = \frac{-2b_2 x^{(2/\alpha)-1} e^{-b_2 x^{2/\alpha}}}{\alpha}$; and $\chi''(x) = \frac{2b_2 e^{-b_2 x^{2/\alpha}}\left(2b_2 x^{\frac{4}{\alpha}-2} + (\alpha-2)x^{\frac{2}{\alpha}-2}\right)}{\alpha^2}$.
For $\alpha > 2$, $\chi''(x) \geq 0$ for $x \geq 0$, and thus $\chi(x)$ is convex for $x \geq 0$.

Then, we apply Jensen's Inequality to get: $\mathrm{E}_X\left[e^{-b_2 X^{2/\alpha}}\right] \geq e^{-b_2 \mathrm{E}[X]^{2/\alpha}}$.

$$\begin{aligned}
\mathrm{E}[X]^{2/\alpha} &= \left\{ \lambda_{\mathrm{MANET}} \phi \int_0^{\mu_c} r^{\alpha+1} e^{-\lambda_{\mathrm{MANET}} r^2 \phi/2} dr \right\}^{2/\alpha} \\
&= (\lambda_{\mathrm{MANET}} \phi/2)^{-1} \left(\Gamma\left(\frac{\alpha}{2}+1\right) - \Gamma\left(\frac{\alpha}{2}+1, \lambda_{\mathrm{MANET}} \mu_c^2 \phi/2\right) \right)^{\frac{2}{\alpha}}.
\end{aligned}$$

$$\begin{aligned}
&\exp\left(-b_2 \mathrm{E}[X]^{2/\alpha}\right) \geq 1-\nu \\
\Rightarrow\ &\Gamma\left(\frac{\alpha}{2}+1, \lambda_{\mathrm{MANET}} \mu_c^2 \phi/2\right) > \Gamma\left(\frac{\alpha}{2}+1\right) - \left(\frac{(\lambda_{\mathrm{MANET}} \phi/2)\log(1-\nu)}{b_2} \right)^{\frac{\alpha}{2}},
\end{aligned}$$

where $\Gamma(a,x) = \int_x^\infty e^{-t} t^{a-1} dt$. Next we use the following approximation for the incomplete Gamma function, when n is integer [319]: $\Gamma(1+n,x) = n! e^{-x} e_n(x)$, where $e_n(x) = 1+x+x^2/2+...+x^n/n!$, for $n = 0,1,2,..$ are the partial sums of the exponential series. Furthermore, since $\lambda_{\mathrm{MANET}} \mu_c^2 \phi/2 \ll 1$ [205], we can safely approximate $e^{-x} \approx 1-x$, and $e_n(x) \approx 1+x$.

8.9 Proof of Lemma 9

Using similar calculations to [280]:

$$
\begin{aligned}
&\mathscr{P}\left(\log\left(1+\max_{e\in\Phi_{\mathrm{E}}}\gamma_{e,o}\right)<\varepsilon\right)\\
&=\mathscr{P}\left(\max_{e\in\Phi_{\mathrm{E}}}\gamma_{e,o}<2^{\varepsilon}-1\right)\\
&\overset{(a)}{=}\mathscr{P}\left(\bigcap_{e\in\Phi_{\mathrm{E}}}\gamma_{e,o}<2^{\varepsilon}-1\right)\\
&\overset{(b)}{=}\mathrm{E}_{\Phi_{\mathrm{E}}}\left[\mathbb{1}\left(\bigcap_{e\in\Phi_{\mathrm{E}}}\gamma_{e,o}<2^{\varepsilon}-1\right)\right]\\
&=\mathrm{E}_{\Phi_{\mathrm{E}}}\left[\prod_{e\in\Phi_{\mathrm{E}}}\mathscr{P}\left(\gamma_{e,o}<2^{\varepsilon}-1|z\right)\right]\\
&=\mathrm{E}_{\Phi_{\mathrm{E}}}\left[\prod_{e\in\Phi_{\mathrm{E}}}\left(1-e^{-P_{\mathrm{E},e}^{-1}(2^{\varepsilon}-1)l(z,o)^{-1}\left(\sigma^2+I_E\right)}\right)\right]\\
&\overset{(c)}{=}\mathrm{E}_{\Phi_{\mathrm{E}}}\left[\prod_{e\in\Phi_{\mathrm{E}}}\left(1-\mathscr{L}_{I_E}\left(P_{\mathrm{E},e}^{-1}(2^{\varepsilon}-1)l(z,o)^{-1}\right)\right)\right]\\
&=\exp\left(-2\pi\lambda_{\mathrm{E}}\int_0^{\infty}\mathrm{E}_{P_{\mathrm{E}}}\left[\mathscr{L}_{I_E}\left(P_{\mathrm{E}}^{-1}(2^{\varepsilon}-1)l(z,o)^{-1}\right)\right]rdr\right)\\
&=\exp\left(-\frac{\lambda_{\mathrm{E}}}{(2^{\varepsilon}-1)^{\frac{2}{\alpha}}\,\mathrm{E}\left[P_{\mathrm{E}}^{\frac{2}{\alpha}}\right]^{-1}\tilde{\Omega}}\right),
\end{aligned}
$$

where (a) comes from the fact that the probability of the most detrimental rate falls below ε is equal to all the rates falling below ε; in (b) the indicator function $\mathbb{1}(A)$ for event A.

References

[1] X. Lin, J. G. Andrews, and A. G., "Spectrum sharing for device-to-device communication in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6727–6740, Dec 2014.

[2] M. A. Dunlap and G. Cook, "Shining on: A primer on solar radiation data," *NASA STI/Recon Technical Report N*, vol. 92, May 1992.

[3] U. Muncuk, "Design optimization and implementation for rf energy harvesting circuits," in *Electrical and Computer Engineering Master's Theses. Paper 93*, Jul 2012. [Online]. Available: http://hdl.handle.net/2047/d20002906

[4] B. Zheng, P. Deng, R. Anguluri, Q. Zhu, and F. Pasqualetti, "Cross-layer codesign for secure cyber-physical systems," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 5, pp. 699–711, May 2016.

[5] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18–23, 2015.

[6] T. Muhonen, "Standardization of industrial internet and iot (iot–internet of things)–perspective on condition-based maintenance," *University of Oulu, Finland*, 2015.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[8] V. Galetić, I. Bojić, M. Kušek, G. Ježić, S. Dešić, and D. Huljenić, "Basic principles of machine-to-

machine communication and its impact on telecommunications industry," in *MIPRO, 2011 Proceedings of the 34th International Convention*, May 2011, pp. 380–385.

[9] Y. Chen and Y. Yang, "Cellular based machine to machine communication with un-peer2peer protocol stack," in *Vehicular Technology Conference Fall (VTC 2009-Fall), 2009 IEEE 70th*, Sept 2009, pp. 1–5.

[10] C. Y. Tu, C. Y. Ho, and C. Y. Huang, "Energy-efficient algorithms and evaluations for massive access management in cellular based machine to machine communications," in *Vehicular Technology Conference (VTC Fall), 2011 IEEE*, Sept 2011, pp. 1–5.

[11] L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, "Mobile cloud computing model and big data analysis for healthcare applications," *IEEE Access*, vol. 4, pp. 6171–6180, 2016.

[12] M. Whaiduzzaman, A. Gani, and A. Naveed, "Pefc: Performance enhancement framework for cloudlet in mobile cloud computing," in *Robotics and Manufacturing Automation (ROMA), 2014 IEEE International Symposium on*, Dec 2014, pp. 224–229.

[13] D. Zhang, Y. Shou, and J. Xu, "The modeling of big traffic data processing based on cloud computing," in *2016 12th World Congress on Intelligent Control and Automation (WCICA)*, June 2016, pp. 2394–2399.

[14] H. Yeo and C. H. Crawford, "Big data: Cloud computing in genomics applications," in *Big Data (Big Data), 2015 IEEE International Conference on*, Oct 2015, pp. 2904–2906.

[15] I. Zinno, L. Mossucca, S. Elefante, C. D. Luca, V. Casola, O. Terzo, F. Casu, and R. Lanari, "Cloud computing for earth surface deformation analysis via spaceborne radar imaging: A case study," *IEEE Transactions on Cloud Computing*, vol. 4, no. 1, pp. 104–118, Jan 2016.

[16] C. W. Tsai, C. F. Lai, M. C. Chiang, and L. T. Yang, "Data mining for internet of things: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 77–97, First 2014.

[17] D. Soldani and A. Manzalini, "Horizon 2020 and beyond: on the 5g operating system for a true digital society," *IEEE Vehicular Technology Magazine*, vol. 10, no. 1, pp. 32–42, 2015.

[18] "Recommendation ITU-R M.2083-0: IMT vision–framework and overall objectives of the future development of IMT for 2020 and beyond," *International Telecommunication Union*, 2015.

[19] L. Liu, G. Miao, and J. Zhang, "Energy-efficient scheduling for downlink multi-user mimo," in *Communications (ICC), 2012 IEEE International Conference on*. IEEE, 2012, pp. 4394–4394.

[20] L. Liu, Y. Yi, J.-F. Chamberland, and J. Zhang, "Energy-efficient power allocation for delay-sensitive multimedia traffic over wireless systems," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 5, pp. 2038–2047, 2014.

[21] C. Zhao, B. T. Wysocki, Y. Liu, C. D. Thiem, N. R. McDonald, and Y. Yi, "Spike-time-dependent encoding for neuromorphic processors," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 12, no. 3, p. 23, 2015.

[22] Y. Yi, Y. Liao, B. Wang, X. Fu, F. Shen, H. Hou, and L. Liu, "Fpga based spike-time dependent encoder and reservoir design in neuromorphic computing processors," *Microprocessors and Microsystems*, vol. 46, pp. 175–183, 2016.

[23] A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the random access channel of lte and lte-a suitable for m2m communications? a survey of alternatives," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 4–16, First 2014.

[24] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5g be?" *IEEE Journal on selected areas in communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[25] G. Neonakis Aggelou and R. Tafazolli, "On the relaying capability of next-generation gsm cellular networks," *IEEE Personal Commun. Mag.*, vol. 8, no. 1, pp. 40–47, Feb 2001.

[26] Z. Jingmei, S. Chunju, W. Ying, and Z. Ping, "Performance of a two-hop cellular system with different power allocation schemes," in *In Proc. IEEE Veh. Tech. Conf. (VTC) 2004-Fall*, vol. 6, Sept 2004, pp. 4538–4542.

[27] V. Sreng, H. Yanikomeroglu, and D. Falconer, "Coverage enhancement through two-hop relaying in cellular radio systems," in *In Proc. of IEEE Wireless Comm. and Net. Conf. (WCNC) 2002*, vol. 2, Mar 2002, pp. 881–885.

[28] H. Chen, L. Liu, N. Mastronarde, L. Ma, and Y. Yi, "Cooperative retransmission for massive mtc under spatiotemporally correlated interference," in *Global Communications Conference (GLOBECOM), 2016 IEEE.* IEEE, 2016, pp. 1–6.

[29] Y. Zhou and W. Zhuang, "Opportunistic cooperation in wireless ad hoc networks with interference correlation," *Peer-to-Peer Networking and Applications*, pp. 1–15, 2015.

[30] G. Nigam, P. Minero, and M. Haenggi, "Spatiotemporal cooperation in heterogeneous cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1253–1265, June 2015.

[31] R. Atat, L. Liu, J. Ashdown, M. Medley, and J. Matyjas, "On the performance of relay-assisted D2D networks under spatially correlated interference," in *IEEE Glob. Comm. Conf., (GLOBECOM)*, Dec 2016, pp. 1–6.

[32] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5g be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, June 2014.

[33] C. Estevez and J. Wu, "Recent advances in green internet of things," in *2015 7th IEEE Latin-American Conference on Communications (LATINCOM)*, Nov 2015, pp. 1–5.

[34] K. Wang, Y. Wang, Y. Sun, S. Guo, and J. Wu, "Green industrial internet of things architecture: An energy-efficient perspective," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 48–54, December 2016.

[35] J. Wu, S. Guo, J. Li, and D. Zeng, "Big data meet green challenges: Greening big data," *IEEE Systems Journal*, vol. 10, no. 3, pp. 873–887, Sept 2016.

[36] Y. Mao, Y. Luo, J. Zhang, and K. B. Letaief, "Energy harvesting small cell networks: feasibility, deployment, and operation," *IEEE Wireless Commun.*, vol. 53, no. 6, pp. 94–101, June 2015.

[37] K. Raychaudhuri and P. Ray, "Privacy challenges in the use of ehealth systems for public health management," *Int. J. E-Health Med. Commun.*, vol. 1, no. 2, pp. 12–23, Apr. 2010. [Online]. Available: http://dx.doi.org/10.4018/jehmc.2010040102

[38] Z. Li and T. J. Oechtering, "Privacy-aware distributed bayesian detection," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1345–1357, Oct 2015.

[39] F. Canelo, B. M. C. Silva, J. J. P. C. Rodrigues, and Z. Zhu, "Performance evaluation of an enhanced cryptography solution for m-health applications in cooperative environments," in *2013 IEEE Global Communications Conference (GLOBECOM)*, Dec 2013, pp. 1711–1716.

[40] A. Rabbachin, A. Conti, and M. Z. Win, "Wireless network intrinsic secrecy," *IEEE/ACM Transactions on Networking*, vol. 23, no. 1, pp. 56–69, Feb 2015.

[41] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 414–454, First 2014.

[42] M. Chi, A. Plaza, J. A. Benediktsson, Z. Sun, J. Shen, and Y. Zhu, "Big data for remote sensing: Challenges and opportunities," *Proceedings of the IEEE*, vol. 104, no. 11, pp. 2207–2219, Nov 2016.

[43] B. Zhang, Z. Zhang, Z. Ren, J. Ma, and W. Wang, "Energy-efficient software-defined data collection by participatory sensing," *IEEE Sensors Journal*, vol. 16, no. 20, pp. 7315–7324, Oct 2016.

[44] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.

[45] B. Guo, C. Chen, D. Zhang, Z. Yu, and A. Chin, "Mobile crowd sensing and computing: when participatory sensing meets participatory social media," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 131–137, February 2016.

[46] M. Chen, S. Mao, and Y. Liu, "Big data: A survey," *Mobile Networks and Applications*, vol. 19, no. 2, pp. 171–209, Apr 2014.

[47] P. Derbekoa, S. Dolevb, E. Gudesb, and S. Sharmab, "Security and privacy aspects in mapreduce on clouds: A survey," *Computer Science Review*, vol. 20, no. 1, pp. 1–28, May 2016.

[48] W. Fan and A. Bifet, "Mining big data: Current status, and forecast to the future," *SIGKDD Explor. Newsl.*, vol. 14, no. 2, pp. 1–5, Apr. 2013. [Online]. Available: http://doi.acm.org/10.1145/2481244.2481246

[49] H. Hu, Y. Wen, T. S. Chua, and X. Li, "Toward scalable systems for big data analytics: A technology tutorial," *IEEE Access*, vol. 2, pp. 652–687, 2014.

[50] P. Jiang, J. Winkley, C. Zhao, R. Munnoch, G. Min, and L. T. Yang, "An intelligent information forwarder for healthcare big data systems with distributed wearable sensors," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1147–1159, Sept 2016.

[51] M. Wang, B. Li, Y. Zhao, and G. Pu, "Formalizing google file system," in *2014 IEEE 20th Pacific Rim International Symposium on Dependable Computing*, Nov 2014, pp. 190–191.

[52] P. Derbekoa, S. Dolevb, E. Gudesb, and S. Sharmab, "Security and privacy aspects in mapreduce on clouds," *Comput. Sci. Rev.*, vol. 20, no. 1, pp. 1–28, May 2016. [Online]. Available: http://dx.doi.org/10.1016/j.cosrev.2016.05.001

[53] A. P. Nugroho, T. Okayasu, M. Horimoto, D. Arita, T. Hoshi, H. Kurosaki, K.-i. Yasuba, E. Inoue, Y. Hirai, M. Mitsuoka *et al.*, "Development of a field environmental monitoring node with over the air update function," *Agricultural Information Research*, vol. 25, no. 3, pp. 86–95, 2016.

[54] D. N. Chorafas, *Business, Marketing, and Management Principles for IT and Engineering*. Boca Raton, FL, USA: Auerbach Publications, June 22 2011.

[55] L. Sanchez, M. Bauer, J. Lanza, R. Olsen, and M. Girod-Genet, "A generic context management framework for personal networking environments," *2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, vol. 00, no. undefined, pp. 1–8, 2006.

[56] J. Wu, I. Bisio, C. Gniady, E. Hossain, M. Valla, and H. Li, "Context-aware networking and communications: Part 1 [guest editorial]," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 14–15, June 2014.

[57] P. Bellavista, A. Corradi, M. Fanelli, and L. Foschini, "A survey of context data distribution for mobile ubiquitous systems," *ACM Comput. Surv.*, vol. 44, no. 4, pp. 24:1–24:45, Sep. 2012. [Online]. Available: http://doi.acm.org/10.1145/2333112.2333119

[58] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[59] J. A. ALLAN, "A review of: "remote sensing: Principles and interpretation". by floyd f. sabins, jr. (san francisco: W. h. freeman, 1978.) [pp. 1+426.]," *International Journal of Remote Sensing*, vol. 1, no. 3, pp. 307–308, 1980.

[60] Y. Ma, H. Wu, L. Wang, B. Huang, R. Ranjan, A. Zomaya, and W. Jie, "Remote sensing big data computing," *Future Gener. Comput. Syst.*, vol. 51, no. C, pp. 47–60, Oct. 2015. [Online]. Available: http://dx.doi.org/10.1016/j.future.2014.10.029

[61] L. Zhang, L. Zhang, and B. Du, "Deep learning for remote sensing data: A technical tutorial on the state of the art," *IEEE Geoscience and Remote Sensing Magazine*, vol. 4, no. 2, pp. 22–40, June 2016.

[62] M. M. U. Rathore, A. Paul, A. Ahmad, B. W. Chen, B. Huang, and W. Ji, "Real-time big data analytical architecture for remote sensing application," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 8, no. 10, pp. 4610–4621, Oct 2015.

[63] L. Wang, H. Zhong, R. Ranjan, A. Zomaya, and P. Liu, "Estimating the statistical characteristics of remote sensing big data in the wavelet transform domain," *IEEE Transactions on Emerging Topics in Computing*, vol. 2, no. 3, pp. 324–337, Sept 2014.

[64] H. Xie, X. Tong, W. Meng, D. Liang, Z. Wang, and W. Shi, "A multilevel stratified spatial sampling approach for the quality assessment of remote-sensing-derived products," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 8, no. 10, pp. 4699–4713, Oct 2015.

[65] M. A. Alsheikh, D. Niyato, S. Lin, H. p. Tan, and Z. Han, "Mobile big data analytics using deep learning and apache spark," *IEEE Network*, vol. 30, no. 3, pp. 22–29, May 2016.

[66] X. Zhang, Z. Yi, Z. Yan, G. Min, W. Wang, A. Elmokashfi, S. Maharjan, and Y. Zhang, "Social computing for mobile big data," *Computer*, vol. 49, no. 9, pp. 86–90, Sept 2016.

[67] M. Tang, H. Zhu, and X. Mao, "A lightweight social computing approach to emergency management policy selection," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 8, pp. 1075–1087, Aug 2016.

[68] M. Parameswaran and A. B. Whinston, "Social computing: An overview," *Communications of the Association for Information Systems*, vol. 19, 2007. [Online]. Available: http://aisel.aisnet.org/cais/vol19/iss1/37/

[69] S. Chang, H. Zhu, W. Zhang, L. Lu, and Y. Zhu, "Pure: Blind regression modeling for low quality data with participatory sensing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 4, pp. 1199–1211, April 2016.

[70] R. B. Messaoud and Y. Ghamri-Doudane, "Fair qoi and energy-aware task allocation in participatory sensing," in *2016 IEEE Wireless Communications and Networking Conference*, April 2016, pp. 1–6.

[71] J. Wang, Y. Wang, D. Zhang, L. Wang, H. Xiong, S. Helal, Y. He, and F. Wang, "Fine-grained multi-task allocation for participatory sensing with a shared budget," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2016.

[72] L. Liu, W. Wei, D. Zhao, and H. Ma, "Urban resolution: New metric for measuring the quality of urban sensing," *IEEE Transactions on Mobile Computing*, vol. 14, no. 12, pp. 2560–2575, Dec 2015.

[73] X. Sun, S. Hu, L. Su, T. F. Abdelzaher, P. Hui, W. Zheng, H. Liu, and J. A. Stankovic, "Participatory sensing meets opportunistic sharing: Automatic phone-to-phone communication in vehicles," *IEEE Transactions on Mobile Computing*, vol. 15, no. 10, pp. 2550–2563, Oct 2016.

[74] C. Xiang, P. Yang, C. Tian, L. Zhang, H. Lin, F. Xiao, M. Zhang, and Y. Liu, "Carm: Crowd-sensing accurate outdoor rss maps with error-prone smartphone measurements," *IEEE Transactions on Mobile Computing*, vol. 15, no. 11, pp. 2669–2681, Nov 2016.

[75] L. Wang, D. Zhang, Z. Yan, H. Xiong, and B. Xie, "effsense: A novel mobile crowd-sensing framework for energy-efficient and cost-effective data uploading," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 12, pp. 1549–1563, Dec 2015.

[76] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, and X. Mao, "Incentives for mobile crowd sensing: A survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 54–67, Firstquarter 2016.

[77] Y. Simmhan, S. Aman, A. Kumbhare, R. Liu, S. Stevens, Q. Zhou, and V. Prasanna, "Cloud-based software platform for big data analytics in smart grids," *Computing in Science Engineering*, vol. 15, no. 4, pp. 38–47, July 2013.

[78] A. Ukil and R. Zivanovic, "Automated analysis of power systems disturbance records: Smart grid big data perspective," in *2014 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*, May 2014, pp. 126–131.

[79] J. Yang, J. Zhao, F. Wen, W. Kong, and Z. Dong, "Mining the big data of residential appliances in the smart grid environment," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, July 2016, pp. 1–5.

[80] L. Liu and Z. Han, "Multi-block admm for big data optimization in smart grid," in *Computing, Networking and Communications (ICNC), 2015 International Conference on*, Feb 2015, pp. 556–561.

[81] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 106–115, Sept 2012.

[82] A. Yassine, A. A. N. Shirehjini, and S. Shirmohammadi, "Smart meters big data: Game theoretic model for fair data sharing in deregulated smart grids," *IEEE Access*, vol. 3, pp. 2743–2754, 2015.

[83] A. A. Yavuz, "An efficient real-time broadcast authentication scheme for command and control messages," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1733–1742, Oct 2014.

[84] V. Nguyen, M. Guirguis, and G. Atia, "A unifying approach for the identification of application-driven stealthy attacks on mobile cps," in *2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2014, pp. 1093–1101.

[85] G. M. Lehto, G. Edlund, T. Smigla, and F. Afinidad, "Protection evaluation framework for tactical satcom architectures," in *MILCOM 2013 - 2013 IEEE Military Communications Conference*, Nov 2013, pp. 1008–1013.

[86] M. M. Rathore, A. Ahmad, A. Paul, and G. Jeon, "Efficient graph-oriented smart transportation using internet of things generated big data," in *2015 11th International Conference on Signal-Image Technology Internet-Based Systems (SITIS)*, Nov 2015, pp. 512–519.

[87] L. Mo, F. Li, Y. Zhu, and A. Huang, "Human physical activity recognition based on computer vision with deep learning model," in *Proc. 2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings*, May 2016, pp. 1–6.

[88] M. S. Zitouni, J. Dias, M. Al-Mualla, and H. Bhaskar, "Hierarchical crowd detection and representation for big data analytics in visual surveillance," in *Systems, Man, and Cybernetics (SMC), 2015 IEEE International Conference on*, Oct 2015, pp. 1827–1832.

[89] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 40, no. 1, pp. 1–12, Jan 2010.

[90] E. Kartsakli, A. S. Lalos, A. Antonopoulos, S. Tennina, M. D. Renzo, L. Alonso, and C. Verikoukis, "A survey on M2M systems for mhealth: A wireless communications perspective," *Sensors*, vol. 14, no. 10, pp. 18 009–18 052, 2014.

[91] M. R. Yuce, "Implementation of wireless body area networks for healthcare systems," *Sensors and Actuators A: Physical*, vol. 162, no. 1, pp. 116 – 129, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0924424710002657

[92] H. Yan, H. Huo, Y. Xu, and M. Gidlund, "Wireless sensor network based e-health system - implementation and experimental results," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 4, pp. 2288–2295, November 2010.

[93] J. F. Martínez, M. S. Familiar, I. Corredor, A. B. García, S. Bravo, and L. López, "Composition and deployment of e-health services over wireless sensor networks," *Mathematical*

and Computer Modelling, vol. 53, no. 3–4, pp. 485 – 503, 2011, telecommunications Software Engineering: Emerging Methods, Models and Tools. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0895717710001548

[94] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 2, pp. 619–641, Second 2014.

[95] D. Cui, "Risk early warning index system in the field of public safety in big data era," in *2015 Sixth International Conference on Intelligent Systems Design and Engineering Applications (ISDEA)*, Aug 2015, pp. 704–707.

[96] U. M. Bhangale, K. R. Kurte, S. S. Durbha, R. L. King, and N. H. Younan, "Big data processing using hpc for remote sensing disaster data," in *2016 IEEE International Geoscience and Remote Sensing Symposium (IGARSS)*, July 2016, pp. 5894–5897.

[97] L. Zhong, K. Takano, Y. Ji, and S. Yamada, "Big data based service area estimation for mobile communications during natural disasters," in *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, March 2016, pp. 687–692.

[98] P. Tin, T. T. Zin, T. Toriu, and H. Hama, "An integrated framework for disaster event analysis in big data environments," in *Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on*, Oct 2013, pp. 255–258.

[99] F. Qu, F. Y. Wang, and L. Yang, "Intelligent transportation spaces: vehicles, traffic, communications, and beyond," *IEEE Communications Magazine*, vol. 48, no. 11, pp. 136–142, November 2010.

[100] L. Xu, J. Li, Y. Shu, and J. Peng, "Sar image denoising via clustering-based principal component analysis," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 52, no. 11, pp. 6858–6869, Nov 2014.

[101] T. C. Chen, S. Sanga, T. Y. Chou, V. Cristini, and M. E. Edgerton, "Neural network with k-means clustering via pca for gene expression profile analysis," in *Proc. Computer Science and Information Engineering, 2009 WRI World Congress on*, vol. 3, March 2009, pp. 670–673.

[102] U. M. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, "Advances in knowledge discovery and data mining," U. M. Fayyad, G. Piatetsky-Shapiro, P. Smyth, and R. Uthurusamy, Eds. Menlo Park, CA, USA: American Association for Artificial Intelligence, 1996, ch. From Data Mining to Knowledge Discovery: An Overview, pp. 1–34. [Online]. Available: http://dl.acm.org/citation.cfm?id=257938.257942

[103] M. Behl and R. Mangharam, "Interactive analytics for smart cities infrastructures," in *Proc. 2016 1st International Workshop on Science of Smart City Operations and Platforms Engineering (SCOPE) in partnership with Global City Teams Challenge (GCTC) (SCOPE - GCTC)*, April 2016, pp. 1–6.

[104] V. Kardeby, "Automatic sensor clustering: connectivity for the internet of things," in *Licentiate thesis, Mid Sweden University, Department of Information Technology and Media*, 2011.

[105] P. Rashidi, D. J. Cook, L. B. Holder, and M. Schmitter-Edgecombe, "Discovering activities to recognize and track in a smart environment," *IEEE Transactions on Knowledge and Data Engineering*, vol. 23, no. 4, pp. 527–539, April 2011.

[106] A. Sotsenko, M. Jansen, M. Milrad, and J. Rana, "Using a rich context model for real-time big data analytics in twitter," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Aug 2016, pp. 228–233.

[107] I. Toure and A. Gangopadhyay, "Real time big data analytics for predicting terrorist incidents," in *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, May 2016, pp. 1–6.

[108] V.-D. Ta, C.-M. Liu, and G. W. Nkabinde, "Big data stream computing in healthcare real-time analytics," in *Proc. 2016 IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, July 2016, pp. 37–42.

[109] A. Daniel, A. Paul, and A. Ahmad, "Near real-time big data analysis on vehicular networks," in *Proc. Soft-Computing and Networks Security (ICSNS), 2015 International Conference on*, Feb 2015, pp. 1–7.

[110] S. Liu, J. Yin, X. Wang, W. Cui, K. Cao, and J. Pei, "Online visual analytics of text streams," *IEEE Transactions on Visualization and Computer Graphics*, vol. 22, no. 11, pp. 2451–2466, Nov 2016.

[111] Y. He, F. R. Yu, N. Zhao, H. Yin, H. Yao, and R. C. Qiu, "Big data analytics in mobile cellular networks," *IEEE Access*, vol. 4, pp. 1985–1996, 2016.

[112] P. Chopade, J. Zhan, K. Roy, and K. Flurchick, "Real-time large-scale big data networks analytics and visualization architecture," in *Proc. Emerging Technologies for a Smarter World (CEWIT), 2015 12th International Conference Expo on*, Oct 2015, pp. 1–6.

[113] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu, "Detection of denial-of-service attacks based on computer vision techniques," *IEEE Transactions on Computers*, vol. 64, no. 9, pp. 2519–2533, Sept 2015.

[114] S. Singh and Y. Liu, "A cloud service architecture for analyzing big monitoring data," *Tsinghua Science and Technology*, vol. 21, no. 1, pp. 55–70, Feb 2016.

[115] Microsoft Download Center, "Project daytona: Iterative mapreduce on windows azure," 2016. [Online]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=52431

[116] Y. Yetis, R. G. Sara, B. A. Erol, H. Kaplan, A. Akuzum, and M. Jamshidi, "Application of big data analytics via cloud computing," in *Proc. 2016 World Automation Congress (WAC)*, July 2016, pp. 1–5.

[117] F. J. Clemente-Castelló, B. Nicolae, K. Katrinis, M. M. Rafique, R. Mayo, J. C. Fernández, and D. Loreti, "Enabling big data analytics in the hybrid cloud using iterative mapreduce," in *Proc. 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*, Dec 2015, pp. 290–299.

[118] M. V. Neves, C. A. F. D. Rose, K. Katrinis, and H. Franke, "Pythia: Faster big data in motion through predictive software-defined network optimization at runtime," in *Proc. Parallel and Distributed Processing Symposium, 2014 IEEE 28th International*, May 2014, pp. 82–90.

[119] S. Islam, J. Keung, K. Lee, and A. Liu, "Empirical prediction models for adaptive resource provisioning in the cloud," *Future Gener. Comput. Syst.*, vol. 28, no. 1, pp. 155–162, Jan. 2012. [Online]. Available: http://dx.doi.org/10.1016/j.future.2011.05.027

[120] R. Buyya, K. Ramamohanarao, C. Leckie, R. N. Calheiros, A. V. Dastjerdi, and S. Versteeg, "Big data analytics-enhanced cloud computing: Challenges, architectural elements, and future directions," in *Proc. Parallel and Distributed Systems (ICPADS), 2015 IEEE 21st International Conference on*, Dec 2015, pp. 75–84.

[121] K. Gai, M. Qiu, and H. Zhao, "Security-aware efficient mass distributed storage approach for cloud systems in big data," in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, April 2016, pp. 140–145.

[122] S. Kang, B. Veeravalli, and K. M. M. Aung, "A security-aware data placement mechanism for big data cloud storage systems," in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, April 2016, pp. 327–332.

[123] K. Sekar and M. Padmavathamma, "Comparative study of encryption algorithm over big data in cloud systems," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, March 2016, pp. 1571–1574.

[124] J. Ni, X. Lin, K. Zhang, Y. Yu, and X. S. Shen, "Secure outsourced data transfer with integrity verification in cloud storage," in *2016 IEEE/CIC International Conference on Communications in China (ICCC)*, July 2016, pp. 1–6.

[125] opendedup, http://opendedup.org/, 2016.

[126] D. T. Meyer and W. J. Bolosky, "A study of practical deduplication," *Trans. Storage*, vol. 7, no. 4, pp. 14:1–14:20, Feb. 2012. [Online]. Available: http://doi.acm.org/10.1145/2078861.2078864

[127] Z. Yan, W. Ding, X. Yu, H. Zhu, and R. H. Deng, "Deduplication on encrypted big data in cloud," *IEEE Transactions on Big Data*, vol. 2, no. 2, pp. 138–150, June 2016.

[128] Y. Gahi, M. Guennoun, and H. T. Mouftah, "Big data analytics: Security and privacy challenges," in *2016 IEEE Symposium on Computers and Communication (ISCC)*, June 2016, pp. 952–957.

[129] S. Rao, S. N. Suma, and M. Sunitha, "Security solutions for big data analytics in healthcare," in *Advances in Computing and Communication Engineering (ICACCE), 2015 Second International Conference on*, May 2015, pp. 510–514.

[130] T. Mahmood and U. Afzal, "Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools," in *Information Assurance (NCIA), 2013 2nd National Conference on*, Dec 2013, pp. 129–134.

[131] D. He, S. Chan, Y. Zhang, C. Wu, and B. Wang, "How effective are the prevailing attack-defense models for cybersecurity anyway?" *IEEE Intelligent Systems*, vol. 29, no. 5, pp. 14–21, Sept 2014.

[132] B. Ristic, "Detecting anomalies from a multitarget tracking output," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 50, no. 1, pp. 798–803, January 2014.

[133] E. Rocha, P. Salvador, and A. Nogueira, "Detection of illicit network activities based on multivariate gaussian fitting of multi-scale traffic characteristics," in *2011 IEEE International Conference on Communications (ICC)*, June 2011, pp. 1–6.

[134] L. Jia, M. Li, P. Zhang, Y. Wu, and H. Zhu, "Sar image change detection based on multiple kernel k-means clustering with local-neighborhood information," *IEEE Geoscience and Remote Sensing Letters*, vol. 13, no. 6, pp. 856–860, June 2016.

[135] J. Murphree, "Machine learning anomaly detection in large systems," in *2016 IEEE AUTOTESTCON*, Sept 2016, pp. 1–9.

[136] Y. Yuan and K. Jia, "A distributed anomaly detection method of operation energy consumption using smart meter data," in *2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, Sept 2015, pp. 310–313.

[137] B. Rao and L. Reddy, "Survey on improved scheduling in hadoop mapreduce in cloud environments," *International Journal of Computer Applications*, vol. 34, no. 9, pp. 29–33, Nov 2011.

[138] C. Liu, S. Ghosal, Z. Jiang, and S. Sarkar, "An unsupervised spatiotemporal graphical modeling approach to anomaly detection in distributed cps," in *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*, April 2016, pp. 1–10.

[139] P. Y. Chen, S. Yang, and J. A. McCann, "Distributed real-time anomaly detection in networked industrial sensing systems," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 6, pp. 3832–3842, June 2015.

[140] Y. Kwon, H. K. Kim, Y. H. Lim, and J. I. Lim, "A behavior-based intrusion detection technique for smart grid infrastructure," in *2015 IEEE Eindhoven PowerTech*, June 2015, pp. 1–6.

[141] H. H. Pajouh, R. Javidan, R. Khayami, D. Ali, and K. K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in iot backbone networks," *IEEE Transactions on Emerging Topics in Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[142] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A lightweight anomaly detection technique for low-resource iot devices: A game-theoretic methodology," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.

[143] N. Tamani and Y. Ghamri-Doudane, "Towards a user privacy preservation system for iot environments: a habit-based approach," in *2016 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, July 2016, pp. 2425–2432.

[144] S. Chen, M. Ma, and Z. Luo, "An authentication framework for multi-domain machine-to-machine communication in cyber-physical systems," in *2015 IEEE Globecom Workshops (GC Wkshps)*, Dec 2015, pp. 1–6.

[145] H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari, and X. Yi, "Secure data analytics for cloud-integrated internet of things applications," *IEEE Cloud Computing*, vol. 3, no. 2, pp. 46–56, Mar 2016.

[146] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home iot devices," in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2015, pp. 163–167.

[147] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Visiot: A threat visualisation tool for iot systems security," in *2015 IEEE International Conference on Communication Workshop (ICCW)*, June 2015, pp. 2633–2638.

[148] D. Takaishi, H. Nishiyama, N. Kato, and R. Miura, "Toward energy efficient big data gathering in densely distributed sensor networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 2, no. 3, pp. 388–397, Sept 2014.

[149] X. Tong, C. Kang, and Q. Xia, "Smart metering load data compression based on load feature identification," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2414–2422, Sept 2016.

[150] S. W. Jun, K. E. Fleming, M. Adler, and J. Emer, "Zip-io: Architecture for application-specific compression of big data," in *Field-Programmable Technology (FPT), 2012 International Conference on*, Dec 2012, pp. 343–351.

[151] L. Tian, H. Wang, Q. Tang, and Y. Zhou, "Surveillance source compression with background modeling for video big data," in *2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (BDCloud-SocialCom-SustainCom)*, Oct 2016, pp. 105–110.

[152] N. Li, J. C. Hou, and L. Sha, "Design and analysis of an mst-based topology control algorithm," *IEEE Transactions on Wireless Communications*, vol. 4, no. 3, pp. 1195–1206, May 2005.

[153] K. Miyao, H. Nakayama, N. Ansari, and N. Kato, "Ltrt: An efficient and reliable topology control algorithm for ad-hoc networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 6050–6058, December 2009.

[154] L. Kong, D. Zhang, Z. He, Q. Xiang, J. Wan, and M. Tao, "Embracing big data with compressive sensing: a green approach in industrial wireless networks," *IEEE Communications Magazine*, vol. 54, no. 10, pp. 53–59, October 2016.

[155] H. Lin, L. Wang, and R. Kong, "Energy efficient clustering protocol for large-scale sensor networks," *IEEE Sensors Journal*, vol. 15, no. 12, pp. 7150–7160, Dec 2015.

[156] A. and H. Y. Kong, "Energy efficient cooperative leach protocol for wireless sensor networks," *Journal of Communications and Networks*, vol. 12, no. 4, pp. 358–365, Aug 2010.

[157] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel, "The cost of a cloud: Research problems in data center networks," *SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 68–73, Dec. 2008. [Online]. Available: http://doi.acm.org/10.1145/1496091.1496103

[158] M. Shojafar, C. Canali, R. Lancellotti, and J. Abawajy, "Adaptive computing-plus-communication optimization framework for multimedia processing in cloud systems," *IEEE Transactions on Cloud Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[159] A. Beloglazov, R. Buyya, Y. C. Lee, A. Zomaya, and Others, "A taxonomy and survey of energy-efficient data centers and cloud computing systems," *Advances in Computers*, vol. 82, no. 2, pp. 47–111, 2011.

[160] H. Chao and J. Wu, "15 - optimizing power saving in cellular networks for machine-to-machine (m2m) communications," in *Machine-to-machine (M2M) Communications*, C. Antón-Haro and M. Dohler, Eds. Oxford: Woodhead Publishing, 2015, pp. 269 – 290. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9781782421023000150

[161] H. Chao, Y. Chen, and J. Wu, "Power saving for machine to machine communications in cellular networks," in *2011 IEEE GLOBECOM Workshops (GC Wkshps)*, Dec 2011, pp. 389–393.

[162] P. Mahadevan, P. Sharma, S. Banerjee, and P. Ranganathan, "A power benchmarking framework for network devices," in *Proceedings of the 8th International IFIP-TC 6 Networking Conference*, ser. NETWORKING '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 795–808.

[163] X. Wang, Y. Yao, X. Wang, K. Lu, and Q. Cao, "Carpo: Correlation-aware power optimization in data center networks," in *INFOCOM, 2012 Proceedings IEEE*, March 2012, pp. 1125–1133.

[164] B. Heller, S. Seetharaman, P. Mahadevan, Y. Yiakoumis, P. Sharma, S. Banerjee, and N. McKeown, "Elastictree: Saving energy in data center networks," in *Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation*, ser. NSDI'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 17–17. [Online]. Available: http://dl.acm.org/citation.cfm?id=1855711.1855728

[165] Y. Zhang and N. Ansari, "Hero: Hierarchical energy optimization for data center networks," *IEEE Systems Journal*, vol. 9, no. 2, pp. 406–415, June 2015.

[166] Y. Han, S. s. Seo, J. Li, J. Hyun, J. H. Yoo, and J. W. K. Hong, "Software defined networking-based traffic engineering for data center networks," in *Network Operations and Management Symposium (APNOMS), 2014 16th Asia-Pacific*, Sept 2014, pp. 1–6.

[167] L. Wang, F. Zhang, K. Zheng, A. V. Vasilakos, S. Ren, and Z. Liu, "Energy-efficient flow scheduling and routing with hard deadlines in data center networks," in *Distributed Computing Systems (ICDCS), 2014 IEEE 34th International Conference on*, June 2014, pp. 248–257.

[168] H. Zhang, K. Chen, W. Bai, D. Han, C. Tian, H. Wang, H. Guan, and M. Zhang, "Guaranteeing deadlines for inter-data center transfers," *IEEE/ACM Transactions on Networking*, vol. PP, no. 99, pp. 1–17, 2016.

[169] J. Zhang, K. Li, D. Guo, H. Qi, W. Li, and Y. Jin, "Mdfs: Deadline-driven flow scheduling scheme in multi-resource environments," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 4, pp. 207–219, Oct 2015.

[170] L. Wang, F. Zhang, J. A. Aroca, A. V. Vasilakos, K. Zheng, C. Hou, D. Li, and Z. Liu, "Greendcn: A general framework for achieving energy efficiency in data center networks," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 1, pp. 4–15, January 2014.

[171] Z. Asad and M. A. R. Chaudhry, "A two-way street: Green big data processing for a greener smart grid," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–11, 2016.

[172] E. Renault, "Parallel execution of for loops using checkpointing techniques," in *Proceedings of the 2005 International Conference on Parallel Processing Workshops*, ser. ICPPW '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 313–319. [Online]. Available: http://dx.doi.org/10.1109/ICPPW.2005.65

[173] L. Mereuta and E. Renault, "Checkpointing aided parallel execution model and analysis," in *Proceedings of the Third International Conference on High Performance Computing and*

Communications, ser. HPCC'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 707–717. [Online]. Available: http://dl.acm.org/citation.cfm?id=2401945.2402023

[174] E. Renault and S. Boumerdassi, "Towards an energy-efficient tool for processing the big data," in *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on*, Aug 2014, pp. 448–452.

[175] A. Katal, M. Wazid, and R. H. Goudar, "Big data: Issues, challenges, tools and good practices," in *Contemporary Computing (IC3), 2013 Sixth International Conference on*, Aug 2013, pp. 404–409.

[176] Z. Asad, M. A. R. Chaudhry, and D. Malone, "Greener data exchange in the cloud: A coding-based optimization for big data processing," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1360–1377, May 2016.

[177] A. Das, C. Lumezanu, Y. Zhang, V. Singh, G. Jiang, and C. Yu, "Transparent and flexible network management for big data processing in the cloud," in *Presented as part of the 5th USENIX Workshop on Hot Topics in Cloud Computing*. Berkeley, CA: USENIX, 2013. [Online]. Available: https://www.usenix.org/conference/hotcloud13/workshop-program/presentations/Das

[178] D. Perino, M. Varvello, and K. P. N. Puttaswamy, "Icn-re: Redundancy elimination for information-centric networking," in *Proceedings of the Second Edition of the ICN Workshop on Information-centric Networking*, ser. ICN '12. New York, NY, USA: ACM, 2012, pp. 91–96. [Online]. Available: http://doi.acm.org/10.1145/2342488.2342508

[179] C. Yan, Y. Song, J. Wang, and W. Guo, "Eliminating the redundancy in mapreduce-based entity resolution," in *Cluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on*, May 2015, pp. 1233–1236.

[180] K. Lee, D. Kim, and I. Shin, "Reboost: Improving throughput in wireless networks using redundancy elimination," *IEEE Communications Letters*, vol. PP, no. 99, pp. 1–1, 2016.

[181] J. Wu, S. Guo, J. Li, and D. Zeng, "Big data meet green challenges: Big data toward green applications," *IEEE Systems Journal*, vol. 10, no. 3, pp. 888–900, Sept 2016.

[182] H. Ayyalasomayajula, E. Gabriel, P. Lindner, and D. Price, "Air quality simulations using big data programming models," in *2016 IEEE Second International Conference on Big Data Computing Service and Applications (BigDataService)*, March 2016, pp. 182–184.

[183] J. Y. Zhu, C. Sun, and V. O. K. Li, "Granger-causality-based air quality estimation with spatio-temporal (s-t) heterogeneous big data," in *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, April 2015, pp. 612–617.

[184] J. Y. Zhu, Y. Zheng, X. Yi, and V. O. K. Li, "A gaussian bayesian model to identify spatio-temporal causalities for air pollution based on urban big data," in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, April 2016, pp. 3–8.

[185] M. Fingas and C. Brown, "Review of oil spill remote sensing," *Marine Pollution Bulletin*, vol. 83, no. 1, pp. 9 – 23, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0025326X14002021

[186] G. Suciu, V. Suciu, C. Dobre, and C. Chilipirea, "Tele-monitoring system for water and underwater environments using cloud and big data systems," in *2015 20th International Conference on Control Systems and Computer Science*, May 2015, pp. 809–813.

[187] Y. Zheng, T. Liu, Y. Wang, Y. Zhu, Y. Liu, and E. Chang, "Diagnosing new york city's noises with ubiquitous data," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ser. UbiComp '14. New York, NY, USA: ACM, 2014, pp. 715–725. [Online]. Available: http://doi.acm.org/10.1145/2632048.2632102

[188] S. Hachem, V. Mallet, R. Ventura, A. Pathak, V. Issarny, P. G. Raverdy, and R. Bhatia, "Monitoring noise pollution using the urban civics middleware," in *Big Data Computing Service and Applications (BigDataService), 2015 IEEE First International Conference on*, March 2015, pp. 52–61.

[189] S. Bera, S. Misra, and M. S. Obaidat, "Energy-efficient smart metering for green smart grid communication," in *2014 IEEE Global Communications Conference*, Dec 2014, pp. 2466–2471.

[190] X. Li, C. P. Bowers, and T. Schnier, "Classification of energy consumption in buildings with outlier detection," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3639–3644, Nov 2010.

[191] C. H. Lee and C. H. Wu, "Collecting and mining big data for electric vehicle systems using battery modeling data," in *Information Technology - New Generations (ITNG), 2015 12th International Conference on*, April 2015, pp. 626–631.

[192] Y. B. Qin, J. Housell, and I. Rodero, "Cloud-based data analytics framework for autonomic smart grid management," in *Proceedings of the 2014 International Conference on Cloud and Autonomic Computing*, ser. ICCAC '14. Washington, DC, USA: IEEE Computer Society, 2014, pp. 97–100. [Online]. Available: http://dx.doi.org/10.1109/ICCAC.2014.39

[193] F. Saremi, O. Fatemieh, H. Ahmadi, H. Wang, T. Abdelzaher, R. Ganti, H. Liu, S. Hu, S. Li, and L. Su, "Experiences with greengps–fuel-efficient navigation using participatory sensing," *IEEE Transactions on Mobile Computing*, vol. 15, no. 3, pp. 672–689, March 2016.

[194] M. Wang and Z. Yan, "Security in D2D communications: A review," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, vol. 1, Aug 2015, pp. 1199–1204.

[195] Y. Gong, Y. Fang, and Y. Guo, "Privacy-preserving collaborative learning for mobile health monitoring," in *2015 IEEE Global Communications Conference (GLOBECOM)*, Dec 2015.

[196] J. Pospiil and M. Novotný, "Evaluating cryptanalytical strength of lightweight cipher present on reconfigurable hardware," in *Digital System Design (DSD), 2012 15th Euromicro Conference on*, Sept 2012, pp. 560–567.

[197] K. Ly, W. Sun, and Y. Jin, "Emerging challenges in cyber-physical systems: A balance of performance, correctness, and security," in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, April 2016, pp. 498–502.

[198] D. Cancila, H. Zaatiti, and R. Passerone, "Cyber-physical system and contract-based design: A three dimensional view," in *Proceedings of the WESE'15: Workshop on Embedded and Cyber-Physical Systems Education*, ser. WESE'15. New York, NY, USA: ACM, 2015, pp. 4:1–4:4. [Online]. Available: http://doi.acm.org/10.1145/2832920.2832924

[199] A. G. Téllez and M. M. Plá, "Multithreaded translation of ptolemy ii designs on multicore platforms,"

in *Complex, Intelligent and Software Intensive Systems, 2008. CISIS 2008. International Conference on*, March 2008, pp. 607–612.

[200] H. Chen and S. Mitra, "Synthesis and verification of motor-transmission shift controller for electric vehicles," in *Cyber-Physical Systems (ICCPS), 2014 ACM/IEEE International Conference on*, April 2014, pp. 25–35.

[201] J. Espinosa, C. Hernandez, J. Abella, D. de Andres, and J. C. Ruiz, "Analysis and rtl correlation of instruction set simulators for automotive microcontroller robustness verification," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2015, pp. 1–6.

[202] M. M. Bersani and M. Garcia-Valls, "The cost of formal verification in adaptive cps. an example of a virtualized server node," in *2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*, Jan 2016, pp. 39–46.

[203] I. R. Goodman, R. P. Mahler, and H. T. Nguyen, *Mathematics of Data Fusion*. Norwell, MA, USA: Kluwer Academic Publishers, 1997.

[204] A. M. Zungeru, L. Ang, S. R. S. Prabaharan, and K. P. Seng, "Radio frequency energy harvesting and management for wireless sensor networks," *CoRR*, vol. abs/1208.4439, 2012. [Online]. Available: http://arxiv.org/abs/1208.4439

[205] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 9, pp. 4788–4799, September 2013.

[206] H. H. Yang, J. Lee, and T. Q. S. Quek, "Heterogeneous cellular network with energy harvesting-based D2D communication," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1406–1419, Feb 2016.

[207] Y. Wang, Y. Liu, C. Wang, Z. Li, X. Sheng, H. G. Lee, N. Chang, and H. Yang, "Storage-less and converter-less photovoltaic energy harvesting with maximum power point tracking for internet of things," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 2, pp. 173–186, Feb 2016.

[208] Drayson Technologies, "RF energy harvesting for the low energy internet of things," 2015, pp. 1–7. [Online]. Available: http://www.getfreevolt.com/

[209] N. Lee, X. Lin, J. G. Andrews, and R. W. Heath, "Power control for D2D underlaid cellular networks: Modeling, algorithms, and analysis," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 1, pp. 1–13, Jan 2015.

[210] G. George, R. K. Mungara, and A. Lozano, "An analytical framework for device-to-device communication in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 11, pp. 6297–6310, Nov 2015.

[211] T. Novlan, H. Dhillon, and J. G. Andrews, "Analytical modeling of uplink cellular networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2669–2679, June 2013.

[212] L. Song, Z. Han, and C. Xu, *Resource Management for Device-to-Device Underlay Communication*. Springer Publishing Company, Incorporated, 2014.

[213] A. H. Sakr and E. Hossain, "Cognitive and energy harvesting-based D2D communication in cellular networks: Stochastic geometry modeling and analysis," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1867–1880, May 2015.

[214] H. ElSawy and E. Hossain, "On stochastic geometry modeling of cellular uplink transmission with truncated channel inversion power control," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4454–4469, Aug 2014.

[215] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, pp. 757–789, Secondquarter 2015.

[216] R. Atat, H. Chen, and L. Liu, "Fundamentals of spatial RF energy harvesting for D2D cellular networks," in *IEEE Global Communications Conference, (GLOBECOM)*, Dec 2016, pp. 1–6.

[217] S. Kim, R. Vyas, J. Bito, K. Niotaki, A. Collado, A. Georgiadis, and M. M. Tentzeris, "Ambient RF energy-harvesting technologies for self-sustainable standalone wireless sensor platforms," *Proceedings of the IEEE*, vol. 102, no. 11, pp. 1649–1666, Nov 2014.

[218] T. Le, K. Mayaram, and T. Fiez, "Efficient far-field radio frequency energy harvesting for passively powered sensor networks," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 5, pp. 1287–1302, May 2008.

[219] X. Kang, Y. C. Liang, H. Garg, and L. Zhang, "Sensing-based spectrum sharing in cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4649–4654, Oct 2009.

[220] M. Haenggi and R. K. Ganti, "Interference in large wireless networks," *Found. Trends Netw.*, vol. 3, no. 2, pp. 127–248, Feb. 2009. [Online]. Available: http://dx.doi.org/10.1561/1300000015

[221] S. Wen, X. Zhu, Y. Lin, Z. Lin, X. Zhang, and D. Yang, "Achievable transmission capacity of relay-assisted device-to-device (D2D) communication underlay cellular networks," in *2013 IEEE 78th Vehicular Technology Conference*, Sept 2013.

[222] A. Laya, K. Wang, A. A. Widaa, J. Alonso-Zarate, J. Markendahl, and L. Alonso, "Device-to-device communications and small cells: enabling spectrum reuse for dense networks," *IEEE Transactions on Wireless Communications*, vol. 21, no. 4, pp. 98–105, August 2014.

[223] L. Karim, A. Anpalagan, N. Nasser, J. N. Almhana, and I. Woungang, "An energy efficient, fault tolerant and secure clustering scheme for M2M communication networks," in *2013 IEEE Globecom Workshops (GC Wkshps)*, Dec 2013, pp. 677–682.

[224] N. Mastronarde, V. Patel, J. Xu, L. Liu, and M. van der Schaar, "To relay or not to relay: Learning device-to-device relaying strategies in cellular networks," *IEEE Transactions on Mobile Computing*, vol. 15, pp. 1569–1585, 2016.

[225] G. Steri, G. Baldini, I. N. Fovino, R. Neisse, and L. Goratti, "A novel multi-hop secure LTE-D2D communication protocol for IoT scenarios," in *2016 23rd International Conference on Telecommunications (ICT)*, May 2016, pp. 1–6.

[226] H. S. Dhillon, Y. Li, P. Nuggehalli, Z. Pi, and J. G. Andrews, "Fundamentals of heterogeneous cellular networks with energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 13, no. 5, pp. 2782–2797, 2014.

[227] C. Capar, D. Goeckel, and D. Towsley, "Broadcast analysis for extended cooperative wireless networks," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5805–5810, Sept 2013.

[228] K. Huang, "Spatial throughput of mobile ad hoc networks powered by energy harvesting," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7597–7612, Nov 2013.

[229] Z. Chen and M. Kountouris, "Distributed SIR-aware opportunistic access control for D2D underlaid cellular networks," in *2014 IEEE Global Communications Conference*, Dec 2014, pp. 1540–1545.

[230] A. Crismani, S. Toumpis, U. Schilcher, G. Brandner, and C. Bettstetter, "Cooperative relaying under spatially and temporally correlated interference," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 10, pp. 4655–4669, Oct 2015.

[231] R. Atat and L. Liu, "On the performance of relay-assisted D2D networks under spatially correlated interference," in *IEEE Global Communications Conference, (GLOBECOM)*, Dec 2016, pp. 1–6.

[232] L. J., L. B., L. B., and C. J., "A resource reuse scheme of D2D communication underlaying LTE network with intercell interference," *Communications and Network*, vol. 5, pp. 187–193, Sep 2013.

[233] S. Andreev, A. Pyattaev, K. Johnsson, O. Galinina, and Y. Koucheryavy, "Cellular traffic offloading onto network-assisted device-to-device connections," *Communications Magazine, IEEE*, vol. 52, no. 4, pp. 20–31, April 2014.

[234] T. Mahmood and U. Afzal, "Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools," in *2013 2nd National Conference on Information Assurance (NCIA)*, Dec 2013, pp. 129–134.

[235] M. Wang and Z. Yan, "Security in D2D communications: A review," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug 2015, pp. 1199–1204.

[236] K. Raychaudhuri and P. Ray, "Privacy challenges in the use of ehealth systems for public health management," *Int. J. E-Health Med. Commun.*, vol. 1, no. 2, pp. 12–23, Apr. 2010. [Online]. Available: http://dx.doi.org/10.4018/jehmc.2010040102

[237] K. Yang, J. Wu, X. Bu, and S. Guo, "Energy-efficient power control for device-to-device communications with max-min fairness," *Proc. IEEE Vehicular Technology Conference (VTC) Fall*, September 2016.

[238] Z. Li and T. J. Oechtering, "Privacy-aware distributed bayesian detection," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1345–1357, Oct 2015.

[239] F. Canelo, B. M. C. Silva, J. J. P. C. Rodrigues, and Z. Zhu, "Performance evaluation of an enhanced cryptography solution for m-health applications in cooperative environments," in *2013 IEEE Global Communications Conference (GLOBECOM)*, Dec 2013, pp. 1711–1716.

[240] X. Lin, J. G. Andrews, and A. Ghosh, "Spectrum sharing for device-to-device communication in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 12, pp. 6727–6740, Dec 2014.

[241] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 996–1019, Third 2013.

[242] A. H. Sakr and E. Hossain, "Cognitive and energy harvesting-based D2D communication in cellular networks: Stochastic geometry modeling and analysis," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1867–1880, May 2015.

[243] H. ElSawy, E. Hossain, and M. S. Alouini, "Analytical modeling of mode selection and power control for underlay D2D communication in cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 11, pp. 4147–4161, Nov 2014.

[244] H. Chen and L. Liu, "Resource allocation for sensing-based device-to-device (D2D) networks," in *2015 49th Asilomar Conference on Signals, Systems and Computers*, Nov 2015, pp. 1058–1062.

[245] H. Chen, L. Liu, T. Novlan, J. D. Matyjas, B. L. Ng, and J. Zhang, "Spatial spectrum sensing-based device-to-device cellular networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7299–7313, Nov 2016.

[246] R. Atat and L. Liu, "On the achievable transmission capacity of secrecy-based D2D cellular networks," in *IEEE Global Communications Conference, (GLOBECOM)*, Dec 2016, pp. 1–6.

[247] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2776–2787, June 2013.

[248] S. Singh, H. S. Dhillon, and J. G. Andrews, "Offloading in heterogeneous networks: Modeling, analysis, and design insights," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2484–2497, May 2013.

[249] H. S. Dhillon, Y. Li, P. Nuggehalli, Z. Pi, and J. G. Andrews, "Fundamentals of heterogeneous cellular networks with energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2782–2797, May 2014.

[250] Y. Lin, W. Bao, W. Yu, and B. Liang, "Optimizing user association and spectrum allocation in hetnets: A utility perspective," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1025–1039, June 2015.

[251] S. Chiu, D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, ser. Wiley Series in Probability and Statistics. Wiley, 2013. [Online]. Available: https://books.google.com/books?id=GCRI8Q-RUEkC

[252] S. Lee, T. Kim, J. Park, S. Lee, and H. Son, "Optimal energy management over solar based energy harvesting sensor network," in *2010 Int. Conf. on Info. and Comm. Tech. Conv. (ICTC)*, Nov 2010, pp. 465–466.

[253] D. K., S. F., and C. B., "Solar power harvesting - modeling and experiences," in *Fachgespräch Sensornetze (FGSN)*, Aug 2009.

[254] P. S. Yu, J. Lee, T. Q. S. Quek, and Y. W. P. Hong, "Traffic offloading in heterogeneous networks with energy harvesting personal cells-network throughput and energy efficiency," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1146–1161, Feb 2016.

[255] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, "Modeling and analysis of k-tier downlink heterogeneous cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 550–560, April 2012.

[256] T. Zhang, J. Zhao, L. An, and D. Liu, "Energy efficiency of base station deployment in ultra dense hetnets: A stochastic geometry analysis," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 184–187, April 2016.

[257] H. S. Jo, Y. J. Sang, P. Xia, and J. G. Andrews, "Heterogeneous cellular networks with flexible cell association: A comprehensive downlink sinr analysis," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3484–3495, October 2012.

[258] J. G. Andrews, S. Singh, Q. Ye, X. Lin, and H. S. Dhillon, "An overview of load balancing in hetnets: old myths and open problems," *IEEE Trans. Wireless Commun.*, vol. 21, no. 2, pp. 18–25, April 2014.

[259] B. Borrelli and L. M. Ritterband, "Special issue on ehealth and mhealth: Challenges and future directions for assessment, treatment, and dissemination," in *American Psychological Association-Health Psychology*, vol. 35, Oct 2015, pp. 1205–1208. [Online]. Available: http://dx.doi.org/10.1037/hea0000323

[260] I. Widya, B. j. V. Beijnum, and A. Salden, "Qoc-based optimization of end-to-end m-health data delivery services," in *2006 14th IEEE International Workshop on Quality of Service*, June 2006, pp. 252–260.

[261] J. Wang, H. Abid, S. Lee, L. Shu, and F. Xia, "A secured health care application architecture for cyber-physical systems," *CoRR*, vol. abs/1201.0213, 2012. [Online]. Available: http://arxiv.org/abs/1201.0213

[262] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 365–378, May 2009.

[263] E. Jovanov, "Wireless technology and system integration in body area networks for m-health applications," in *IEEE Engineering in Medicine and Biology 27th Annual Conference*, Jan 2005, pp. 7158–7160.

[264] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE Journal on Selected Areas in Comm.*, vol. 27, no. 4, pp. 400–411, May 2009.

[265] S. Tennina, E. Kartsakli, F. Graziosi, M. Santos, A. S. Lalos, A. Antonopoulos, P. V. Mekikis, M. D. Renzo, L. Alonso, and C. Verikoukis, "An energy efficient protocol architecture for m-health systems," in *2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Dec 2014, pp. 144–148.

[266] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[267] M. M. Haque, A. S. K. Pathan, and C. S. Hong, "Securing u-healthcare sensor networks using public key based scheme," in *Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on*, vol. 2, Feb 2008, pp. 1108–1111.

[268] A. Solanas, A. Martinez-Balleste, P. A. Perez-Martinez, A. F. d. l. Pena, and J. Ramos, "m-carer: Privacy-aware monitoring for people with mild cognitive impairment and dementia," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 19–27, September 2013.

[269] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in *Proceedings of the 1st ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments*, ser. HealthNet '07. New York, NY, USA: ACM, 2007, pp. 7–12. [Online]. Available: http://doi.acm.org/10.1145/1248054.1248058

[270] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J. P. Hubaux, "Secure neighborhood discovery: a fundamental element for mobile ad hoc networking," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132–139, February 2008.

[271] S. Čapkun, L. Buttyán, and J.-P. Hubaux, "Sector: Secure tracking of node encounters in multi-hop wireless networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, ser. SASN '03. New York, NY, USA: ACM, 2003, pp. 21–32. [Online]. Available: http://doi.acm.org/10.1145/986858.986862

[272] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, vol. 3, March 2003, pp. 1976–1986 vol.3.

[273] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Network and Distributed System Security Symposium Conference Proceedings: 2004*, Internet Society. San Diego: Director of Conferences and Education, Internet Society, 1775 Wiehle Avenue, Suite 102, Reston, Virginia 20190-5108, U.S.A., Feb. 2004.

[274] K. B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*, Sept 2007, pp. 331–340.

[275] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[276] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Communications Letters*, vol. 3, no. 3, pp. 289–292, June 2014.

[277] H. Wu, X. Tao, Z. Han, N. Li, and J. Xu, "Secure transmission in misome wiretap channel with multiple assisting jammers: Maximum secrecy rate and optimal power allocation," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 775–789, Feb 2017.

[278] R. Atat, L. Liu, and Y. Yi, "Privacy protection scheme for ehealth systems: A stochastic geometry approach," in *2016 IEEE Global Communications Conference (GLOBECOM'16)*, Dec. 2016.

[279] R. Atat and L. Liu, "On the achievable transmission capacity of secrecy-based D2D cellular networks," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[280] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. on Communications*, vol. 63, no. 1, pp. 229–242, Jan 2015.

[281] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 6, pp. 2006–2021, June 2014.

[282] Y. Pei, Y. c. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over miso cognitive radio channels," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1494–1502, April 2010.

[283] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, October 2013.

[284] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, Aug 2010.

[285] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1128–1138, June 2016.

[286] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 839–850, May 2014.

[287] F. Menichelli, R. Menicocci, M. Olivieri, and A. Trifiletti, "High-level side-channel attack modeling and simulation for security-critical systems on chips," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 3, pp. 164–176, July 2008.

[288] R. Gentz, S. X. Wu, H. T. Wai, A. Scaglione, and A. Leshem, "Data injection attacks in randomized gossiping," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 2, no. 4, pp. 523–538, Dec 2016.

[289] A. R. Syed and K. L. A. Yau, "On cognitive radio-based wireless body area networks for medical applications," in *Computational Intelligence in Healthcare and e-health (CICARE), 2013 IEEE Symposium on*, April 2013, pp. 51–57.

[290] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 996–1019, Third 2013.

[291] W. Sun, Y. Ge, Z. Zhang, and W. C. Wong, "An analysis framework for inter-user interference in ieee 802.15.6 body sensor networks: A stochastic geometry approach," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, 2015.

[292] H. Wirtz, R. Backhaus, R. Hummen, and K. Wehrle, "Establishing mobile ad-hoc networks in 802.11 infrastructure mode," in *Proceedings of the 6th ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization*, ser. WiNTECH '11, no. 2. New York, NY, USA: ACM, 2011, pp. 89–90.

[293] "IEEE 802.11: Wireless LAN medium access control (MAC) and physical layer (PHY)," 1999.

[294] H. ElSawy, E. Hossain, and M. S. Alouini, "Analytical modeling of mode selection and power control for underlay D2D communication in cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 11, pp. 4147–4161, Nov 2014.

[295] H. ElSawy, E. Hossain, and S. Camorlinga, "Spectrum-efficient multi-channel design for coexisting ieee 802.15.4 networks: A stochastic geometry approach," *IEEE Transactions on Mobile Computing*, vol. 13, no. 7, pp. 1611–1624, July 2014.

[296] F. Baccelli, J. Li, T. Richardson, S. Subramanian, X. Wu, and S. Shakkottai, "On optimizing csma for wide area ad-hoc networks," in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2011 International Symposium on*, May 2011, pp. 354–359.

[297] M. Haenggi, "Mean interference in hard-core wireless networks," *IEEE Communications Letters*, vol. 15, no. 8, pp. 792–794, August 2011.

[298] S. Srinivasa and M. Haenggi, "Combining stochastic geometry and statistical mechanics for the analysis and design of mesh networks," *Ad Hoc Networks*, vol. 13, pp. 110–122, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2011.03.014

[299] M. Haenggi, "On distances in uniformly random networks," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3584–3586, Oct 2005.

[300] G. Geraci, M. Wildemeersch, and T. Q. S. Quek, "Energy efficiency of distributed signal processing in wireless networks: A cross-layer analysis," *IEEE Transactions on Signal Processing*, vol. 64, no. 4, pp. 1034–1047, Feb 2016.

[301] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, Inc., 2013.

[302] M. Dehghan, D. L. Goeckel, M. Ghaderi, and Z. Ding, "Energy efficiency of cooperative jamming strategies in secure wireless networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 9, pp. 3025–3029, September 2012.

[303] N. Zhang, N. Lu, R. Lu, J. W. Mark, and X. Shen, "Energy-efficient and trust-aware cooperation in cognitive radio networks," in *2012 IEEE International Conference on Communications (ICC)*, June 2012, pp. 1763–1767.

[304] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Location-based secure transmission for wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 7, pp. 1458–1470, July 2015.

[305] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2764–2775, August 2011.

[306] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2776–2787, June 2013.

[307] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1850–1863, September 2013.

[308] N. Li, X. Tao, H. Chen, and H. Wu, "Secrecy outage probability for the multiuser downlink with several curious users," in *2016 IEEE Wireless Communications and Networking Conference*, April 2016, pp. 1–5.

[309] F. Baccelli and B. Błaszczyszyn, "Stochastic geometry and wireless networks: Volume i theory," *Foundations and Trends® in Networking*, vol. 3, no. 3–4, pp. 249–449, 2010. [Online]. Available: http://dx.doi.org/10.1561/1300000006

[310] K. Choi, S. Choi, and J. H. Yun, "On the joint distribution of aggregate interference at multiple wireless receivers," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 3, pp. 1355–1362, March 2013.

[311] Z. Chen, C. X. Wang, X. Hong, J. S. Thompson, S. A. Vorobyov, X. Ge, H. Xiao, and F. Zhao, "Aggregate interference modeling in cognitive radio networks with power and contention control," *IEEE Transactions on Communications*, vol. 60, no. 2, pp. 456–468, February 2012.

[312] A. Ghasemi and E. S. Sousa, "Interference aggregation in spectrum-sensing cognitive wireless networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 41–56, Feb 2008.

[313] N. Rajewsky, L. Santen, A. Schadschneider, and M. Schreckenberg, "The asymmetric exclusion process: Comparison of update procedures," *Journal of Statistical Physics*, vol. 92, no. 1, pp. 151–194, 1998. [Online]. Available: http://dx.doi.org/10.1023/A:1023047703307

[314] H. S. Dhillon, Y. Li, P. Nuggehalli, Z. Pi, and J. G. Andrews, "Fundamentals of heterogeneous cellular networks with energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 13, no. 5, pp. 2782–2797, May 2014.

[315] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, May 2007, pp. 107–115.

[316] J.-S. Ferenc and Z. Neda, "On the size distribution of poisson-voronoi cells," *Physica A-Statistical Mechanics And Its Applications*, vol. 385, no. 2, pp. 518–526, 2007.

[317] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 3122–3134, November 2011.

[318] N. Lee, X. Lin, J. G. Andrews, and R. W. H. Jr., "Power control for D2D underlaid cellular networks: Modeling, algorithms and analysis," *CoRR*, vol. abs/1305.6161, 2013. [Online]. Available: http://arxiv.org/abs/1305.6161

[319] W. Gautschi, "The incomplete gamma functions since tricomi," in *In Tricomi's Ideas and Contemporary Applied Mathematics, Atti dei Convegni Lincei, n. 147, Accademia Nazionale dei Lincei*, 1998, pp. 203–237.