UNIVERSITÀ
DEGLI STUDI
DI FERRARA

- EX LABORE FRUCTUS -

DEPARTMENT OF ENGINEERING

Ph.D. in Sciences of Engineering

Cycle XXX

Coordinator: Prof. Stefano Trillo

Context-Aware Massive Wireless Networks: Modeling and Design

Disciplinary Area ING-INF/03

Ph.D. Candidate: **Giovanni Chisci**

Advisor: **Prof. Andrea Conti**

Co-Advisor: **Prof. Lorenzo Mucchi**

February 2018

"Controlling what we do is being free."

Daft Punk

Abstract

The smart world era is yet to come with all its multitude of applications including smart cities, smart industry, smart agricolture, smart energy, and smart mobility. Internet of things (IoT) is the underlaid paradigm for the realization of the smart world by the interconnection of a massive multitude of heterogeneous devices. Along with the tremendously increasing user-generated traffic, next-era wireless communications will face unprecedented demands also in terms of machine-generated traffic, according to the arising big data applications and the development of sophisticate cyber physical systems (CPSs).

To unlock the potentials and reap the benefits of IoT, scalable, reliable, resilient, secure, and efficient wireless networking platforms are required. In this Ph.D. dissertation we introduce the concept of massive wireless network (MWN), which is of particular importance in the fifth generation (5G) ecosystem. With MWN we intend a network where the wireless terminals may include autonomous terrestrial vehicles, unmanned arial vehicles, sensors, actuators, alarms, cameras, smart phones, computers, and smart physical objects (things). Each type of these coexisting wireless terminals has unique features in terms of complexity, traffic demand, battery life, propagation environment, and quality of service (QoS) constraints, which all have to be considered within the design and operation of MWNs. Catering for such highly diverse demands within the MWNs is the first step towards smart world and big data era.

This Ph.D. dissertation tackles the scalability, reliability, and security of the MWN by developing stochastic models for network analysis and design. Stochastic modeling is the way to not focus on a specific network, but to account for all networks with common features in a stochastic sense, to achieve fundamental results and provide general guidelines for the design. Nevertheless, our models include important contex-informations, specifically

spatial (topology) and temporal (delay, traffic) ones, to assess the location-dependent performance of the network. This is required to properly develop the surging IoT and CPSs. The enormous opportunities that this new era can bring to industrial and vertical markets including, public safety, logistics, well-being, and smart cities, are beyond imagination. Furthermore, the applications enabled by IoT create new business opportunities through developing specific products and solutions.

The dissertation is organized as follows: in Chapter 1 we show the vision of the *smart world* era and we describe the challenges of next-generation wireless networking, in Chapter 2 we face the scalability and reliability problem in wireless networks, in Chapter 3 we tackle the problem of intrinsic secrecy in wireless networks, and in Chapter 4 we conclude the dissertation providing some future research challenges.

Contents

List of Figures

List of Tables

List of Abbreviations

Acronyms

3GPP third generation partnership project

5G fifth generation

C-RAN cloud radio access network

c.f. call for

CCDF complementary cumulative distribution function

CDF cumulative distribution function

CPS cyber physical system

D2D device-to-device

DoS denial of service

DTMC discrete-time Markov chain

ER eavesdropping receiver

ERN eavesdropping receiver network

F-ALOHA frequency ALOHA

FHN full homogeneous networ

FIFO first-in-first-out

FIN full inhomogeneous network

H2M human-to-machine

HD high density

HetNet heterogeneous network

HNS1 hybrid network scenario 1

HNS2 hybrid network scenario 2

HPPP homogeneous Poisson point process

i.f.f. if and only if

i.i.d. independent and identically distributed

IES interference engineering strategy

II intentional interferer

IIN intentional interferer network

IoT Internet of things

IP Internet protocol

IPPP inhomogeneous Poisson point process

KC k^{th} closest

KPI key performance indicator

LD low density

LMSR local maximum secrecy rate

LNSRD local network secrecy rate density

LNSTD local network secrecy throughput density

LoRa long-range radio

LPWAN low-power wide area network

LR legitimate receiver

LRN legitimate receiver network

LT legitimate transmitter

LTE long term evolution

LTN legitimate transmitter network

M2M machine-to-machine

MAM matrix analytic method

MIMO multiple-input-multiple-output

mm-wave millimeter wave

MS maximum SIR

MSR maximum secrecy rate

MWN massive wireless network

NB-IoT narrowband IoT

NSI non-smart informed

NSNI non-smart non-informed

NSR network secrecy rate

NST network secrecy throughput

PBN Poisson bipolar network

PDF probability density function

PGFL probability generating functional

PIN partial inhomogeneous network

PPP Poisson point process

QBD quasi-birth-and-death

QoE quality of experience

QoS quality of service

RV random variable

s.t. such that

SI smart informed

SINR signal-to-interference-plus-noise ratio

SIR signal-to-interference ratio

SNI smart non-informed

SOP secrecy outage probability

UMTS universal mobile telecommunications service

V2V vehicle-to-vehicle

VNI virtual network indexing

w.r.t. with respect to

WIPT wireless transfer of information and power

WSN wireless sensor network

Chapter 1

Introduction

The next generation wireless communication networks are key enablers for supplying big data, automating cites, and bridging physical and cyber worlds, thus leading to the upcoming *smart world era*, for a revolution in connectivity, networking, monitoring, surveillance, automation, decision making, control, and business opportunities. This Ph.D. dissertation tackles the foundation of next generation wireless communications by introducing massive wireless networks (MWNs). In particular we provide a context-aware modeling for the analysis and design of reliable, resilient, efficient, and secure networks and of algorithms for their operation (see Fig. 1.1).

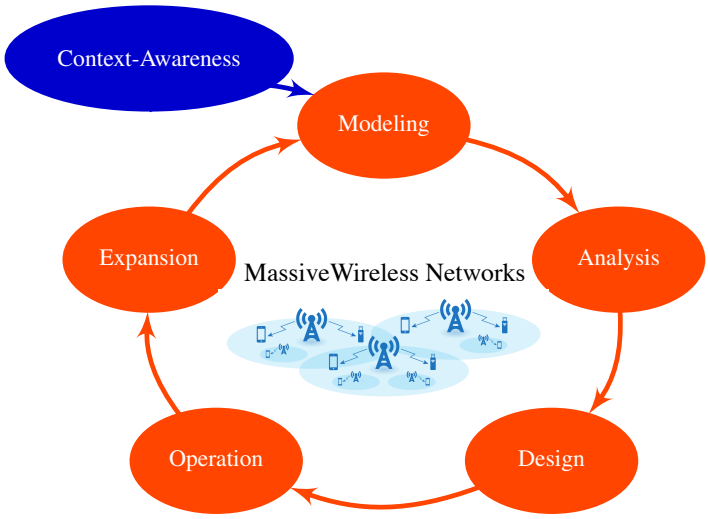

Figure 1.1: Framework for the development of future generation wireless networks.

1.1 Big Picture: The Smart World Era and Next Generation Wireless Communications

The Smart World

The *smart world* is a human-centric concept, a vision, that is to use data for decision making and automation, to improve the life of human beings, preserve the environment, and reduce the costs to achieve such goals [1]. This concept has its derivations in the different aspects of the life and society, which are smart agriculture [2–4], smart industry [5–7], smart energy [8–10], smart homes [11–13], smart retail [14–16], smart mobility [17–19], smart health [20–22], smart government [23–25], smart education [26, 27], which in the literature are well'known as sectors of the *smart cities* [28] (see Fig. 1.2).

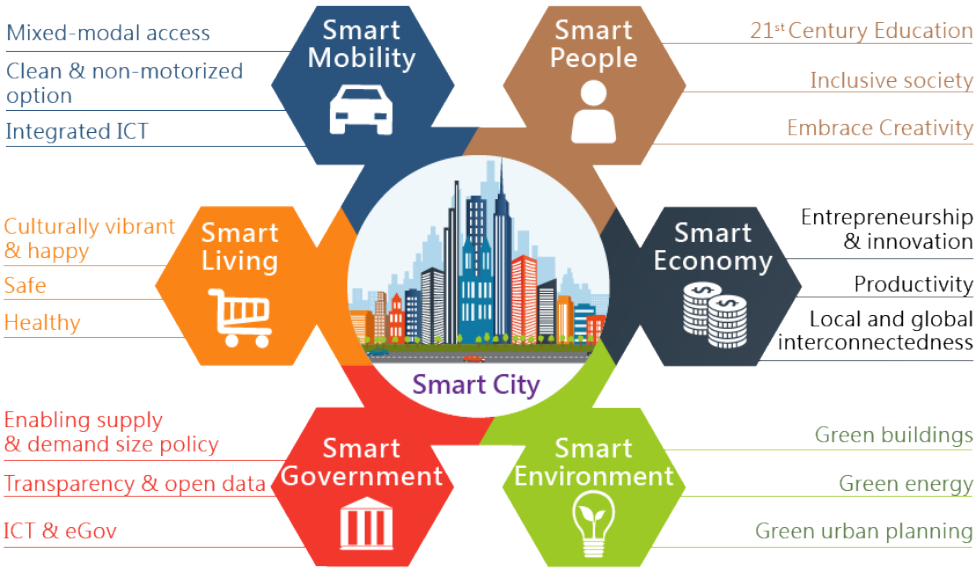

Figure 1.2: The applications of the smart city. This picture can be found at www.smartcity.org.hk.

There exist in the literature formal definitions for smart cities [29]; we chose to adopt the following to include both the data-centric and the communication-centric points of view: a smarty city uses a combination of data collection, processing, and disseminating technologies in conjunction with networking and computing technologies and data security and privacy measures thus encouraging the innovation of applications to promote the overall quality of life for its citizens, preserve the environment, and reduce the costs of living

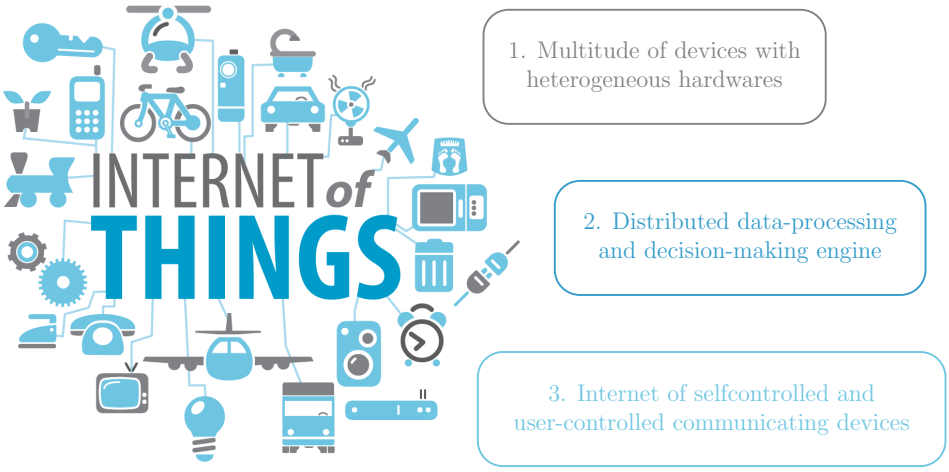

Figure 1.3: IoT layers. This figure has been created starting from the IoT logo, which can be found at www.silicon.it.

by covering dimensions including utilities, health, transportation, economy, entertainment, and government services [1].

Enabling the Smart World: the Role of IoT

In general, the attribute *smart* indicates the fact that data are used to automatize processes and improve their efficiency within a networking framework, such that (s.t.) the monitoring of operations is always possible. The answer to the demand of a smart networking platform for the realization of smart cities is provided by the surging Internet of things (IoT), which is the paradigm for the interconnection of a massive number of devices of heterogeneous type (things) [30]. The nature of the IoT is mainly threefold as depicted in Fig. 1.3:

1. a distributed multitude of devices with sensing and actuating capabilities (device-centric point of view);

2. a distributed powerful data processing and decision-making engine (data-centric point of view); and

3. an internet of communicating devices either selfcontrolled or controlled by users (communication-centric point of view).

The definition of IoT has been changing over time along with the evolution of the technology. Lately, it has become: "The IoT allows people and

things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service" [31]. In the near future, almost all active devices will have an Internet interface. This vision enforces data scientists to provide solutions for the inevitable challenge of how to process the large amount of data coming from things, and how to make sense of the raw extracted data. With the proliferation of wireless devices (e.g., mobile phones, wireless sensors and actuators, wireless smart meters, unmanned vehicles and drones), wireless networks become a global information infrastructure incurring a fast escalation of data volume known as big data [32].

Being "Smart": Big Data Applications

IoT will enable the implementation of big data [33, 34] applications; that is to analyze, process, and make inference on large and heterogeneous data sets; for the realization of more smart and green environments [32, 35, 36]. Incorporating sensors and cloud computing, sensor-cloud [37] is a very powerful system for users to achieve big data in smart cities. In particular, a massive amount of data will be sensed in cities and gathered by a multitude of ubiquitous sensors (e.g., temperature, humidity, pressure, light, and video sensors) and further transmitted to the cloud via sinks. The big data will be then stored and processed by powerful data centers and delivered to users on-demand. Hence, with sensor clouds, users are able to access to data anytime and anywhere if there is any network connection.

5G and Massive Wireless Networks

To support the requirements of the IoT, a new-generation wireless networking platform is needed to answer to the unprecedented demands in terms of reliability, latency, bandwith, rate, coverage [38]. In that regards, technological solutions are evolving towards the development of fifth generation (5G) wireless networks, e.g., millimeter wave (mm-wave) communications, massive multiple-input-multiple-output (MIMO) systems, dense small cells, moving cells, heterogeneous networks (HetNets), cloud radio access network (C-RAN), smart antennas, beamforming [39].

Hence, when compared to state-of-the-art wireless networks, the next-era networks, which we denote as MWNs, are discriminated with the following characteristics:

- a massive multitude of wireless terminals in their totality;
- a significant heterogeneity in the type of the devices in terms of complexity, battery life, sensing, actuating, computational, communica-

tion, energy harvesting, and mobility capabilities; thus including autonomous and non autonomous terrestrial vehicles, unmanned arial vehicles, sensors, actuators, alarms, cameras, smart phones, base stations, computers, i.e., smart physical objects or things;

- a wide range of applications including monitoring, automation, security, city management, commerce, public safety, health care, energy distribution, transportation; and

- an extensive variety of requirements ranging from reliability, low-delay, fault-intolerancy, resiliency, security, energy-efficiency.

Catering for such extremely dense and highly diverse demands within the MWNs is the first-mile towards smart world and big data era and the focus of this Ph.D. thesis dissertation. MWNs are key enablers to reap the next-era unprecedented opportunities leading to a better, safer, and more efficient everyday life. While the potentials are limitless and span every industrial sector, in the following we mention two examples for the sake of illustration.

- **Automotive:**
  - **Fact:** Every year, 1.3 million die and 50 million are injured on road accidents [40,41]. The US by itself witnesses over 30,000 fatal crashes per year [40, 42]. From an economical perspective, the annual global cost of car accidents is far beyond $500 million [40]. Besides accidents, traffic congestions have tremendous negative effects on the economy. According to *The Economist*, a study has estimated the total economical cost of traffic jams in 2013 across four countries, including the US, to be around $200 billion [43].
  - **Vision:** Imagine a smart vehicular system where vehicles can communicate together and access real time traffic data. Such system will lead to optimal utilization of the road infrastructure and autonomous driving with no human errors, which will significantly improve road safety and efficiency. Incorporating vehicles into the world of connected physical objects will further increase the level of context-awareness[1] and improve safety and efficiency. In addition to the information about locations, speeds, and directions of proximate vehicles, each vehicle will also be aware of pedestrians, cyclists, pets, real time road statuses, and traffic alerts (e.g., accidents, congestions, icy/de-iced roads).

[1]In that regard, it is worth to mention the importance of localization and navigation systems, which allow to track context informations as position and speed of objects by wireless signals. This allow to make context-aware decisions [44–48].

- **Health-care:**
  - **Fact:** Health-care is a major source of national expenditure that imposes significant burden on the US economy. Late and wrong diagnosis are two major existing issues that negatively impact the health of individuals and significantly contribute to the cost of health-care. *The Washington Post* recently reported that almost every individual in the US gets a late or wrong diagnosis at least once in their lives [49].
  - **Vision:** Imagine a system where accurate and ubiquitous health monitoring is viable. The real time health conditions and vital information of each patient become accessible for doctors and nurses, alleviating the necessity for long waiting queues for regular check-ups. Early diagnosis becomes a matter of developing appropriate over the top application. The availability and ubiquity of the patient vital signals can dramatically improve diagnosis efficiency and expedite the patients release from hospitals. Besides reducing infection risks and improving psychological state of patients, early release will also decrease health-care expenditures.

The aforementioned brief examples just highlight the social and economic impact of the technologies enabled by MWNs on individuals and society. The added values that MWNs can bring to each industrial and vertical market, including public safety, logistics, well-being, industrial automation, smart cities, etc., are beyond imagination [50, 51]. Besides improving the efficiency of these sectors, the applications enabled by MWNs create new business opportunities through developing specific products and solutions.

1.2 The Problems and the Goals

1.2.1 The scalability problem of the IoT

The connectivity in the MWNs plays a major role in enabling an interoperable access and interconnections among heterogeneous smart objects. In fact, in smart cities, infrastructured and infrastructureless telecommunication networks can and have to provide a reliable and efficient delivery of services and high-quality information under diverse communication quality of service (QoS) and user quality of experience (QoE) constraints. This can be achieved by leveraging a large number of digital devices along with the involvement of various technologies such as wireless sensor networks (WSNs),

machine-to-machine (M2M), vehicle-to-vehicle (V2V), and device-to-device (D2D) communications, with or without the support of the cellular network.

During the last years, wireless networks have been experiencing a tremendous growth of user-generated traffic demand. With the increasing popularity of smart devices, Internet protocol (IP)-based networks have become a part of everyday life. As a result, a set of new, user-oriented mobile multimedia applications, like mobile video conferencing, video streaming, and e-healthcare are coming up. Several rapid changes respond to new capacity demands resulting from the massive data growth over the last ten years especially posed by video. In fact, since 2012 video traffic is more than half of the global mobile traffic [52]. The actual video resolution capability of handsets has increased to 4K, which will need a data rate of 15.4 Mbps per user (using H.265 profile 5.1, 4K resolution at 64 fps and Chroma ratio 4:4:4) [53]. An average mobile user is expected to download around 1 terabyte of data annually by 2020 [54]. The demand of contents will keep on increasing at high rates, beyond forecasts. In fact, the mobile traffic per year is expected to increase to 291.8 exabytes by 2019 [55]. Statistics reveal that global mobile traffic esperienced around 70% growth in 2014 [52]. Only 26% smartphones (of the total global mobile devices) are responsible for 88% of total mobile data traffic [52]. Cisco's virtual network indexing (VNI) forecasts that mobile networks will have more than half of connected devices as smart devices by 2019.

Next to the satisfaction of the enormous user-generated traffic demand, there is a surging seek for city automations, which are intrinsically delay- and fault-intolerant applications [56]. Thus, wireless networks will face unprecedented traffic demands in terms of M2M communications. For long time, multihop short-range communications with mesh topology have been considered as highly suitable to implement IoT services involving M2M communications [57–59].

Standards such as ZigBee and Bluetooth provide examples of very low-power standards but with limited coverage, which is and obstacle for applications that require urban-wide coverage or place-&-play type of connectivity [60].[2]

Hence, after experimentations of some smart city services the need for something different arose. In that regard cellular networks play a role because of their ability to provide ubiquitous coverage to IoT nodes. Nevertheless, latest cellular standards, i.e., universal mobile telecommunications service (UMTS) and long term evolution (LTE), were not designed to accomodate

[2]It is possible to connect an IoT device just placing it in a desired location and turning it on.

the IoT and its demand for massive and sporadic M2M type of communications [61–63]. In fact the control signaling and the access network could be the bottlenecks of IoT-enabled cellular networks, thus opening new scalability challenges towards the development of 5G networks.

To unlock the potentials and reap the benefits of MWNs, a scalable, reliable, and efficient wireless networking platform is required. This motivated industry to release several new technologies, such as 3GPP narrowband IoT (NB-IoT), long-range radio (LoRa), SIGFOX, and Weightless, that operate towards low-power wide area networks (LPWANs). LPWANs are solutions that exploit sub-gigahertz unlicensed frequency bands, characterized by star topologies and long-range communications [64, 65]. These are solutions standing in between short-range communications with mesh topologies and long-range cellular-based narrowband communications.

However, due to the lack of precise mathematical models for MWNs, it is unknown to which extent such networks can support in terms of devices density and what QoS level they can guarantee. Further, there is no rigorous framework to design such networks and optimally tune the network parameters to fulfill given key performance indicators (KPIs) constraints. Current mathematical models are inadequate for MWNs due to their myopic focus either on the macroscopic scale interactions between devices or the microscopic behavior of nodes. On one extreme, macroscopic scale frameworks utilize stochastic geometry to account for mutual interference between devices with saturated buffers. Stochastic geometry analysis provides spatially averaged performance metrics that overlook important temporal KPIs (e.g., delay) and fail to give per-node performance characterization. On the other extreme, traffic-aware microscopic scale frameworks utilizes queuing theory with collision model (or vulnerability region models) to account for the interactions between neighboring devices. Simplistic collision models fail to capture realistic signal-to-interference-plus-noise ratio (SINR) interactions between devices, overlook the potential of spatial frequency reuse, and cannot relate the KPIs to the network density, which are fundamentals in MWNs.

Thus our approach is to combine stochastic geometry and queuing theory to account for important spatial and temporal contextual informations to devise a novel spatiotemporal modeling for the analysis and design of MWNs. The dissertation of this part of the work is given in Chapter 2.

1.2.2 The security problem in the next-generation networks

Security is one of the main challenges for next-generation wireless networks [66–68]. The variety of applications, scenarios, devices, and communication types make the security problem. A security system must provide *confidentiality*, *integrity*, *authentication*, and *non-repudiation* of the information. Consider security in the IoT, in particular the M2M type of communications involving sensing and actuating devices; such systems might be exposed to attacks such as denial of service (DoS) and, in this context, availability and resilience are important factors. Also requirements such as privacy, anonymity, liability, and trust will be vital for the development of IoT applications involving social networking, and internet-integrated sensing and actuating devices. In some applications involving M2M or human-to-machine (H2M), data such as sensor measurements or control signals for automations need to be transmitted with privacy in order to prevent unwanted listeners from overhearing classified informations, e.g., about commercial exercises, or cyber physical system (CPS) behavior and operation (e.g., how many times during a day a smart lock is opened) which might also hinder citizen's privacy. The work in [66] cathegorize the citizen's privacy into five areas, which are location privacy, privacy of state of body and mind, privacy of social life, privacy of behavior and actions, privacy of media. Information privacy is a challenge falling within the area of the *privacy of media*. That is, the privacy of images, video, audio, and other data such as biometric signals or account numbers of a person [69].

In the third chapter of this Ph.D. dissertation we consider the problem of the transmission of confidential information, to address both the privacy of the machine- and user-generated traffic in the MWN. First, some preliminary considerations need to be made, which lead to state our approach and methodology:

- wireless communication networks are particularly vulnerable to eavesdropping due to the intrinsically brodcast radio channel;
- the devices involved in the communication might have limited computational capabilities, which hinders the utilization of criptography;
- the advent of quantum computing will undermine in the near future the trustworthiness of criptography-based secrecy systems, due to the possibility of launching brute force attacks in small times;
- MWNs will suffer from an enormous overhead and signaling because of

the key distribution mechanism, which burdens the usage of criptography in massively dense networks;

- physical layer security is a promising approach to complement criptography with an additional layer of security; and
- the phisical properties of the wireless communication medium, offer the possibility to provide some level of message confidentiality with the help of proper coding and processing.

Starting form Shannon's information-theoretic principle of perfect secrecy [70], several techniques that exploit artificial noise, network interference, and legitimate node cooperation have been proposed [71–75]. Such works assume that provided impaired eavesdropping channels, a certain amount of transmission rate can be delivered with theoretically certain confidentiality. Stochastic geometry have been extensively used to assess the average secrecy level by including spatial and protocol context-informations [76–86]. Such works account for the node spatial distribution by homogeneous point processes for tractability, which allow to determine the averaged performance. We propose to fill a modeling gap by accounting for *inhomogeneous networks* rather that homogeneous ones. In fact information confidentiality have to be guaranteed at every location in order to provide the network with security. Our work assume more fine-grain description of the network spatial-model to inspect the location-dependent secrecy performance. We utilize probability theory, communication theory, information theory and stochastic geometry to include the context-information. The dissertation is provided in Chapter 3.

1.2.3 Mathematical Theory of MWNs

Due to the broadcast nature of the wireless channel, the mandatory (i.e., due to spectrum scarcity) spatial frequency reuse, and the propagation characteristics of the wireless medium, the performance of large-scale networks are characterized by the SINR at the receiving devices. The SINR is a fundamental performance metric for two reasons: 1) it captures the topology-dependent spatial interactions among the network elements and devices, which are manifested in the aggregate network interference; and 2) it determines several important QoS metrics such as throughput, error probability, and capacity. Several studies have been carried out to evaluate the performance of communications with disturbances and interference [87–92].

Stochastic geometry is a branch of applied probability that is instrumental to study and develop the theory of large-scale networks [93–96]. Specifically,

it is fundamental to include the spatial context-informations that are needed to characterize the aggregated interference and the SINR in wireless stocastic networks, which are objects of this Ph.D. dissertation. Stochastic geometry based analysis has been extensively applied for ad-hoc, Wi-Fi, and cellular networks, where the positions of the the network elements (e.g., cellular base stations and Wi-Fi access points) and devices are modeled by stochastic point processes [97–100].

There exist in the literature solid contributions to the mathematical theory of stochastic large-scale networks, specially for Poisson point processes (PPPs) [93,101,102]. A comprehensive characterization of aggregate network interference and its subsequent effect on SINR-dependent QoS metrics (e.g., bit error rate, symbol error rate, outage probability, and ergodic capacity) are presented in [103, 104]. The spectral properties of aggregate network interference are characterized in [104, 105]. The impact of spectrum overlap between narrowband networks and ultra-wideband networks is studied in [106, 107]. Spectrum sharing between primary and secondary networks is characterized in [108]. A theoretical framework for interference alignment in large-scale networks is developed in [109, 110]. Last but not least, interference engineering for physical layer security in stochastic large-scale networks is presented in [74, 76, 77, 110–112]. A comprehensive tutorial on the use of stochastic geometry for modeling, analysis, and design of cellular networks is presented in [96].

Despite its instrumental role in large-scale networks, stand-alone stochastic geometry models are inadequate for MWNs. A majority of stochastic geometry models in the literature adopt spatially averaged snapshot-based analysis for devices with saturated buffers, which implicitly 1) assume that the devices are always active, 2) are oblivious to the different time scales of transmission, fading variation, and topology dynamics (i.e., due to mobility), and 3) overlook the temporal and contextual aspects of MWNs. Hence, the analysis can neither account for the sporadic traffic patterns, the diverse applications, nor capture the per-device microscopic performance (e.g., queue activity), all of which are crucial for MWNs. It is shown in [113, 114] that spatially averaged performance metrics can be misleading to network designers as it hides important details about the underlying variance regarding the devices performance. Note that the analysis in [113, 114] is very specific to preemptive ad-hoc and cellular network models and should be extended to much richer sets of topologies that may appear in MWNs. To overcome the aforementioned deficiencies, this Ph.D. dissertation goes beyond state-of-the-art and develop mathematical theory of large-scale networks that incorporates the macroscopic and microscopic features of MWNs and account for the statistical measures of the KPIs rather than spatial averages. This

will be achieved by combining queueing theory and stochastic geometry, and by introducing the notion of *spatial traffic density*. The developed theory will provide fundamentally new understanding of the MWN operation by accounting for the interplay between the traffic generation, transmission rates, medium access protocol, and spatiotemporally correlated aggregate network interference (call for (c.f.) Chapter 2). Capturing this interplay leads to accurate mathematical models for MWN design.

For what regard the intrinsic secrecy aspects of MWNs, it is in the scope of this Ph.D. dissertation to provide a different perspective on the location-dependent secrecy performance. In fact, we account for inhomogeneous network models, to understand the continuous spatial variation of the KPIs such as secrecy rate and throughput (c.f. Chapter 3).

1.2.4 Organization of the Ph.D. Dissertation

The Ph.D. dissertation is further organized in following three parts: Chapter 2 addresses the spatiotemporal modeling and design of MWNs, Chapter 3 develops the intrinsic secrecy analysys for inhomogeneous networks, and Chapter 4 provides final remarks and future research challenges.

Chapter 2

Spatiotemporal Modeling of Uncoordinated Massive Networks

2.1 Preliminaries

2.1.1 Big Picture

Massive wireless networks; consisting of many wireless nodes including sensors, actuators, machines, vehicles, drones, and many other smart objects (things); will significantly contribute to the big data supply and automation of the foreseen smart world. Realizing such massive wireless connectivity is an important foundation for the IoT and CPSs,[1] which are emerging in different sectors including smart cities, public safety, health-care, autonomous vehicles, etc. [30,115]. Each of these sectors will entail massively many connected things, hereafter denoted as nodes,[2] which are required to communicate with each other and/or connect to the Internet with a given QoS. For instance, public safety and autonomous driving may require ultra-reliable low-latency communications. Other sectors, such as monitoring and automation, may require massive number of connections with flexible constraints in terms of delay and reliability. Consequently, developing a scalable wireless networking platform that is able to accommodate the traffic generated from massively many nodes with different QoS requirements is mandatory to unlock the potential and reap the benefits of the foreseen smart era.

Spectrum access and reuse are among the fundamental challenges for MWNs. The massive number of nodes, heterogeneous node types, sporadic

[1] While IoT and CPSs involve different layers of the protocol stack, MWNs focus on the wireless communications at the physical and medium access layers.

[2] MWNs may include users equipment, sensors, machines, and vehicles.

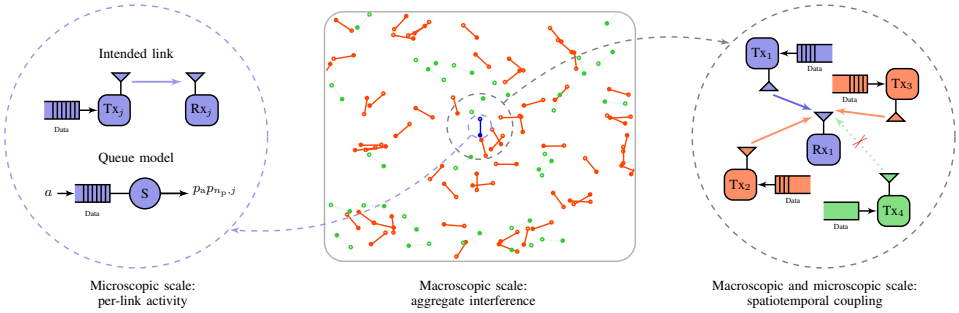

Figure 2.1: Network model illustrating the macroscopic and microscopic scales of the proposed spatiotemporal model.

traffic patterns, wide-spatial existence, and different QoS requirements impose several new challenges to wireless communications and networking. In the context of IoT, there are several evolving low-power wireless technologies, such as LoRa, SigFox, On-Ramp Wireless, and Weightless, to address such challenges [116]. The third generation partnership project (3GPP) LTE standard also provides solutions for accommodating IoT traffic within the cellular networks such as device-to-device communications, machine-to-machine communications, and narrowband IoT (NB-IoT) [117]. Each of these technologies provides innovative solutions in terms of energy efficiency, spectrum sharing, and traffic prioritization to fulfill the diverse IoT requirements. However, uncoordinated spectrum access is a common ground in all of these technologies [63, 116–118]. In particular, variations of ALOHA, with or without carrier sensing, are used to either transmit data and/or request scheduling. However, it is well known that ALOHA performance degrades as the number of nodes grows [63, 116, 117], which raises the following fundamental questions; i) how to quantify the scalability of ALOHA for MWNs in terms of per-node traffic intensity, node density, and required transmission rate; and ii) how to ensure a stable network operation and guarantee a desirable performance for a given percentile of the MWN. The answer of these questions gather into a rigorous framework for the design and implementation of IoT and CPS. It will also determine the extent to which current network solutions can accommodate from the surging IoT and CPS traffic.

2.1.2 Related works and Motivation

To characterize the scalability and design spectrum access strategies, mathematical models that capture the essences of MWNs are required. Conventionally, mathematical models that involve interacting queues are uti-

lized to study and design spectrum access strategies [119–122]. However, in [119–122], a pessimistic collision model is used to account for the interactions among the queues. Interacting queues are also used to design scheduling techniques over fading channels in wireless systems [123, 124]. However, the work in [123, 124] is limited to a single server model that allows single transmission per time slot. A realistic SINR-based two-queue interactions is modeled in [125, 126] for interference and broadcast channels. However, the model in [125, 126] cannot be generalized to the MWN. The authors in [127, 128] propose an integrated graph and queuing theory model that captures the interactions among the queues of neighbor nodes. However, the methodology presented in [125,126] fails to capture the aggregate effect from non-neighbors, which may by significant in MWNs. In conclusion, the models in [119–128] abstract spatial and/or physical layer attributes (e.g., SINR capture model, the wide spatial existence, the aggregate network interference, etc.), which are fundamental for MWNs.

Spatial and physical layer attributes are usually captured via stochastic geometry models [93, 101, 102, 113, 129, 130], where the nodes spatial locations are modeled via point processes. Radio propagation and fading models are used in conjunction with point process theory to model the concurrent transmissions that lead to mutual interference among the spatially coexisting nodes. By averaging over all spatial realizations of the point process and channel fading, spatially averaged SINR-dependent performance metrics are obtained such as bit/symbol error probabilities [103, 131], transmission rates [104, 132], outage probabilities [107, 133], and information secrecy [74, 76, 134]. Nevertheless, the stochastic geometry works in [74, 76, 93, 101–104, 107, 113, 129–134] are based on the spatially-averaged analysis which overlooks the temporal attributes such as traffic generation, queue occupation, and the resulting node activities, as well as queueing performance metrics such as service delay and queuing length, which are also fundamentals to characterize MWNs.

To jointly account for the temporal, spatial, and physical layer attributes in large-scale wireless networks, recent studies integrate stochastic geometry and queueing theory [135–140]. For instance, studies for energy harvesting-powered communications in wireless networks are presented in [135, 136]. However, the queueing theory is utilized to model the battery level dynamics while assuming saturated data buffers. The spatiotemporal interactions between nodes with non-saturated data buffers are studied in [137–140]. However, the analysis in [137, 138] assumes high mobility scenarios, which allow to consider the network topology at every time slot as randomly and independently generated from the considered point process and, hence, spatial averages for the performance characterization. The works in [138,139] utilize

a dominant system model where all nodes are always active even if they have empty queues, which can be quite pessimistic for MWNs. The work in [140] is confined to uplink traffic for IoT-enabled cellular networks where every queue in the network behaves like the *typical queue*, which is not generally true for MWNs.

2.1.3 Contribution

By a joint utilization of stochastic geometry and queueing theory this chapter, which is in part presented in [1, 4], presents a holistic spatiotemporal modeling for MWNs (c.f. Fig. 2.1). On the macroscopic scale, stochastic geometry is used to account for the mutual interference among the coexisting nodes. On the microscopic scale, queueing theory is used to account for the per-node buffer state and transmission protocol state. Our solution challenges the intrinsic interdependency between the macroscopic- and microscopic-scale analysis, i.e., allows to characterize the aggregate interference and the related quantities also accounting for the node activities due to their buffer occupations and protocol states. Since transmission and fading occur at a much smaller time scale than the spatial dynamics (e.g., due to mobility), the spatial realization of the network is assumed as static. To go beyond the existing literature, which uses spatially averaged metrics to characterize the performance, we utilize the concept of the meta distribution of SINR [113, 114] to account for the diverse qualities of the links coexisting in the network and classify such links into different QoS classes. To this end, we quantify the network scalability via the percentile-based Pareto frontiers of the stability regions in terms of per-node traffic intensity, node density, target transmission rate, and uncoordinated access persistence. Operating beyond stability regions means that the nodes buffer overflow with probability one and the network is not scalable to accommodate the MWN generated traffic. The developed framework is used to design networks with stable operation and/or a desired QoS level, which are ensured for a target percentile of the MWN. The contributions of this chapter can be summarized as follows

- developing a mathematical model that accounts for the intricate spatiotemporal interactions in the MWN and quantifies the network scalability in terms of spatiotemporal traffic density and target percentile performance.

- presenting the γ-*stability* (γ-*operativity*) Pareto-frontiers that define the ranges of the network parameters and design variables that guarantee stable-queues (target QoS level) for γ% of the MWN;

- proposing different uncoordinated access protocols that balance the tradeoffs between transmission deferral, power-ramping, and persistence to improve the γ-*stability* and/or γ-*operativity* of ALOHA.

2.1.4 Notation and Organization

Notation

Along the chapter we use the serif font, e.g., v, for random variables (RVs) and the roman font, e.g., v for their instantiation. Vectors are bolded, e.g., $\mathbf{v}$ and $\boldsymbol{v}$; matrices are bolded and uppercase, e.g., $\mathbf{V}$ and $\boldsymbol{V}$; and sets are uppercase, e.g., Ω and $\mathit{\Omega}$. The notation $[\cdot]^\top$ is used to denote the transpose operator and the notation $\boldsymbol{V}^{[i,j]}$ is used to denote the i^{th}-row j^{th}-column element. $\boldsymbol{V}^{[:,j]}$ and $\boldsymbol{V}^{[i,:]}$ are used to denote all elements in the j^{th} column and all elements in the i^{th} row, respectively. With a slight abuse of notation we use $v^{[i]}$ to denote the i^{th} element $\boldsymbol{v}^{[i]}$ of a vector. The functions $f_{\mathsf{v}}(\cdot)$, $F_{\mathsf{v}}(\cdot)$, $\bar{F}_{\mathsf{v}}(\cdot)$, and $\mathcal{L}_{\mathsf{v}}(\cdot)$ denote the probability density function (PDF), cumulative distribution function (CDF), complementary cumulative distribution function (CCDF), and legitimate transmitter (LT) of the RV v,[3] respectively. We denote by $\mathbb{P}\{\cdot\}$, $\mathbb{E}\{\cdot\}$, $\mathbb{P}^{!\circ}\{\cdot\}$, and $\mathbb{E}^{!\circ}\{\cdot\}$ the probability, expectation, Palm probability, and Palm expectation, respectively. With the over-bar we denote the complement operator, i.e., $\bar{v} = 1 - v$, and $\lceil \cdot \rceil$ denotes the ceiling function.

Organization

We present the system model and the analysis methodology in Section 2.2; Section 2.3 presents the macroscopic analysis corresponding to the stochastic geometry part of the framework by characterizing the meta distribution of the SINR of a network of interacting queues; Section 2.4 presents the microscopic analysis which corresponds to the queuing theory part of the framework through the discrete-time Markov chain (DTMC) representation of the buffer and protocol states; Section 2.5 presents the iterative solution of the spatiotemporal model, introduces the KPIs, and presents the notions of network stability and target operativity; Section 2.6 discusses numerical results and shows a design case study; Section 2.7 provides final remarks, thus, concluding the chapter.

[3]From now till the rest of the chapter we will abuse the terminology "LT of the RV v" for the LT of its PDF.

2.2 System Model

For the sake of organized presentation, the spatial and physical layer models are first presented and then followed by the temporal and medium-access control (MAC) layer attributes.

2.2.1 Spatial and Physical Layer Parameters

This chapter considers MWNs in which nodes are scattered in $\mathbb{R}^2$ according to a Poisson bipolar network (PBN) [143, Def. 5.8]. That is, the potential transmitters belongs to a PPP $\Pi = \{\mathbf{y}_j \in \mathbb{R}^2, j \in \mathbb{N}_+\}$, with intensity λ and each transmitter communicates with a dedicated receiver located at a fixed distance φ in a uniformly random orientation. A realization of the PBN is shown in Fig. 2.1. For simplicity, we consider the unbounded path loss model $\ell(r) = r^{-2\eta}$, where r is the propagation distance and η is the amplitude loss exponent. We account for a Rayleigh fading environment with unit mean channel power gains. All channels gains are assumed to be independent and identically distributed (i.i.d.) from one location to another and from one time slot to another. Each transmission is defined by a frequency-power pair and at every channel access frequency ALOHA (F-ALOHA) is used to uniformly and randomly select one of the N_{c} frequency channels [144, 145]. The transmission power is selected among N_{p} different power levels $\mathcal{P} = \{P_1, P_2, \ldots, P_{N_{\mathrm{p}}}\}$ according to the employed power-ramping scheme, which is described in the next section.

2.2.2 Temporal Parameters and Queuing Model

We consider a discrete-time system with slot duration of T_{s} seconds. As shown in Fig. 2.1, each transmitter has a buffer that stores data received from higher layers. An i.i.d. Bernoulli traffic generation model, with per-slot probability of $0 < a < 1$, is assumed at each buffer which induces i.i.d. geometric inter arrival times. At each time slot, transmitters with non-empty buffers employ a slotted F-ALOHA protocol with transmission probability $\breve{p}_{\mathrm{a}} \triangleq p_{\mathrm{a}}/N_{\mathrm{c}}$ to access any of the N_{c} channels and probability p_{a} to access any channel. Upon a channel access, each transmitter operates at a fixed rate of $R_{\mathrm{t}} = W \log(1+\theta)$ [bits/second]. Hence, a packet size of $T_{\mathrm{s}} R_{\mathrm{t}}$ [bits/packet] is successfully transmitted if the SINR at the intended receiver exceeds θ.

Packets are transmitted according to a first-in-first-out (FIFO) rule and only successfully received packets are dropped from the transmitter buffers. Otherwise, the packet is kept in the buffer until successful transmission. When a transmission failure occurs, the node changes the transmission power

for the next channel access according to the employed power-ramping scheme. Starting from the initial power level P_1, a node uses the same transmission power P_i for up to N_t consecutive retransmissions,[4] where N_t is a design variable. If the transmission is still unsuccessful, the next power level P_{i+1} is utilized for the next N_t retransmissions. Ramping-up (i.e., $P_{i+1} > P_i$) is the greedy choice to prioritize delayed transmissions at the expense of increasing the interference level and deteriorating the success probability of other nodes' packets. In contrast, ramping-down ($P_{i+1} < P_i$) is the altruistic choice that reliefs the interference level in the network, especially in regions where packets are subjected to high delays. The retransmission protocol is restarted either upon a transmission success or after exploring all power levels (i.e., the counter tracking the retransmissions is cleared and the node restarts the transmission from P_1). The power-ramping protocol state, namely the phase, is defined by both the physical (power) and logical (retransmission) states leading to $M = N_\mathrm{p}N_\mathrm{t}$ transmission phases. We assume that positive and negative transmission acknowledgements are sent over a delay-free and error-free control channel.

Since the time scale of fading and packet transmission is much smaller than that of the spatial dynamics (e.g., due to mobility) [146], it is assumed that the realization of the network nodes remains static during the network operation. That is, an arbitrary, but fixed, network realization $\mathsf{\Pi} = \mathit{\Pi}$ of the PBN is considered over the temporal domain and only channel fading, queue states, node activities, channel access, and transmission powers change from one time slot to another.

2.2.3 Methodology

The operation of the aforementioned network involves intricate and interdependent interactions among the spatially distributed queues. As shown in Fig. 2.1, the macroscopic effect of the network interference and the microscopic effect of the per-node behavior are interrelated. Furthermore, the static network topology leads to a location-dependent packet departure probability of each queue (c.f. Fig. 2.2). That is, the packet departure probability of a given link depends on i) the location of the intended receiver relative to the other transmitters, ii) the employed power by the intended transmitter, and iii) the status of all other transmitters (i.e., activity and transmission powers). For a given network realization $\mathsf{\Pi} = \mathit{\Pi}$, let $n_\mathrm{p} \in \mathcal{N}_\mathrm{p} = \{1, 2, \ldots, N_\mathrm{p}\}$ be the power level index and $\mathsf{z}_{n_\mathrm{p},j}$ be the SINR at the intended receiver of

[4]Note that consecutive retransmissions do not necessarily occur in consecutive time slots due to the ALOHA random backoff.

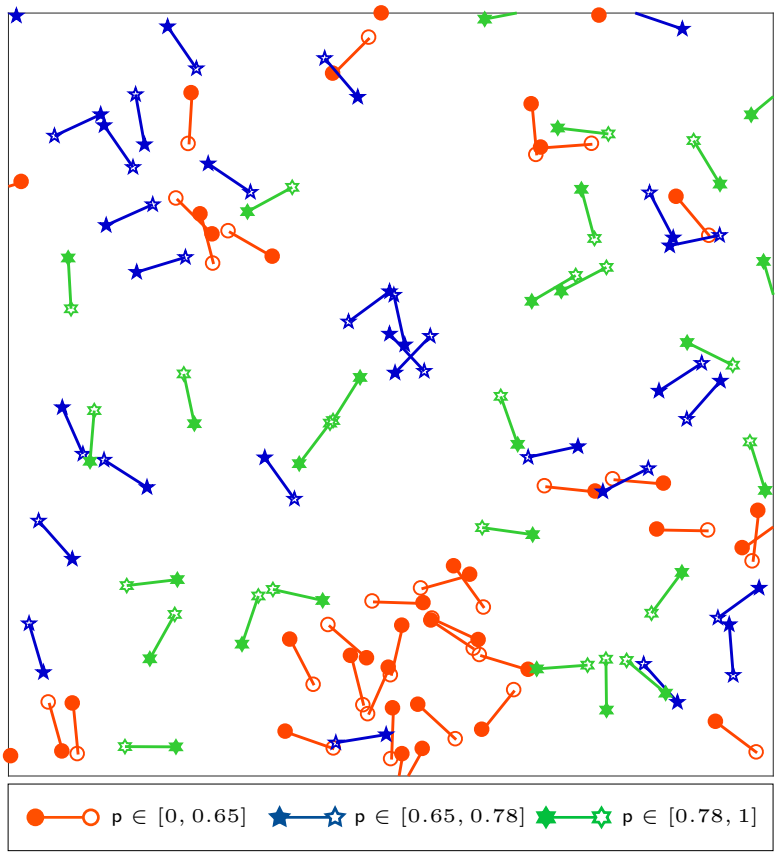

Figure 2.2: Three QoS-classes classification for the packet departure probability within a realization of the PBN operating with ALOHA for $N_{\mathrm{c}} = N_{\mathrm{p}} = N_{\mathrm{t}} = 1$, where the filled (empty) shapes represent transmitters (receivers). The green hexagrams, blue pentagrams, and red circles represent the high ($\mathsf{p} > 0.78$), medium ($0.65 < \mathsf{p} < 0.78$), and low ($\mathsf{p} < 0.65$) QoS links, respectively.

the transmitter located at $\boldsymbol{y}_j \in \Pi$ when operating with the power level $P_{n_{\mathrm{p}}}$. Further, let $p_{n_{\mathrm{p}},j}$ be the probability that $\mathsf{z}_{n_{\mathrm{p}},j}$ is greater than θ. A departure from the queue abstracting the j^{th} wireless link as in Fig. 2.1 occurs upon the joint independent events of channel access and transmission success, i.e., with probability $p_{\mathrm{a}} p_{n_{\mathrm{p}},j}$. Although Π is fixed, the values $p_{n_{\mathrm{p}},j}$ along the network can be considered as realizations of the RV $\mathsf{p}_{n_{\mathrm{p}}}$. The distribution of $\mathsf{p}_{n_{\mathrm{p}}}$ is denoted as the meta distribution of the SINR with CDF $F_{\mathsf{p}_{n_{\mathrm{p}}}}(\phi) \triangleq \mathbb{P}\{\mathsf{p}_{n_{\mathrm{p}}} < \phi\}$ which indicates the fraction of links in the network having a success probability smaller than ϕ [113]. Further, let $\boldsymbol{\rho}_j \in \mathcal{P} \cup \{0\}$ for $j \in \mathbb{N}^+$ be i.i.d.

RVs modeling the nodes' physical state and $\boldsymbol{w}_{\boldsymbol{\rho}} = [w^{[0]}, w^{[1]}, \ldots, w^{[N_\mathrm{p}]}$ be the spatially averaged steady-state distribution of $\boldsymbol{\rho}_j$ for all j, where $w^{[0]}$ is the probability of being idle due to empty buffer and $w^{[i]}$ is the probability of having non-empty buffer while being in any of the retransmission phases of the power level P_i. To analyze the considered MWN, we consider the following steps as shown in Fig. 2.3:

(a) Macroscopic analysis by stochastic geometry as a function of $\boldsymbol{w}_{\boldsymbol{\rho}}$.

- Find the moments of $\mathsf{p}_{n_\mathrm{p}}$, where the b^{th} moment is denoted as M_{b,n_p}, for every power level $n_\mathrm{p} \in \mathcal{N}_\mathrm{p}$.
- For every power level $n_\mathrm{p} \in \mathcal{N}_\mathrm{p}$, apply the moment matching to approximate the meta distribution $f_{\mathsf{p}_{n_\mathrm{p}}}(\cdot)$ via the beta distribution.
- Discretize the meta distribution $f_{\mathsf{p}_{n_\mathrm{p}}}(\cdot)$ of each power level n_p into N equiprobable values corresponding to N QoS-classes. Construct the success probabilities matrix $\boldsymbol{D}^{[n_\mathrm{p},i]} = d_{n_\mathrm{p}}^{[i]}$, where each row of $\boldsymbol{D}$ contains the success probabilities for all QoS-classes using the same power level $n_\mathrm{p} \in \mathcal{N}_\mathrm{p}$ and each column contains the success probabilities for all power levels within the same QoS-class $n \in \mathcal{N}$.

(b) Microscopic analysis by queueing theory as a function of $\boldsymbol{D}$

- Use the arrival probability a and the class dependent success probabilities $\boldsymbol{D}^{[:,n]}$ to find the marginal steady-state distribution $\boldsymbol{\pi}_n = [\pi_n^{[0]}, \pi_n^{[1]}, \ldots, \pi_n^{[N_\mathrm{p}]}]$ of node physical states for each class $n \in \mathcal{N}$, where $\pi_n^{[0]}$ is the probability of being idle due to empty buffer and $\pi_n^{[n_\mathrm{p}]}$ is the probability of being in a retransmission phase that employs the power level n_p.
- Aggregate the per-class states to get the overall steady-state marginal distribution $\boldsymbol{w}_{\boldsymbol{\rho}}$ of node physical states, where $w^{[i]} = \frac{1}{N}\sum_{n=1}^{N} \pi_n^{[i]}$.

(c) Iterative solution for $\boldsymbol{w}_{\boldsymbol{\rho}}$ and $\boldsymbol{D}$

- Initialize $\boldsymbol{w}_{\boldsymbol{\rho}}$ such that $\boldsymbol{w}_{\boldsymbol{\rho}} \cdot \mathbf{1} = 1$, where $\mathbf{1}$ is a column vector of ones.
- Solve the system of equations generated by stochastic geometry and queueing theory analysis to find the steady-state $\boldsymbol{w}_{\boldsymbol{\rho}}$ and $\boldsymbol{D}$ by following the iterative algorithm shown in Fig. 2.3 until convergence.

The macroscopic stochastic geometry analysis in (a) is presented in Section 2.3, the microscopic queueing theory analysis in (b) is presented in Section 2.4, and the iterative solution in (c) is presented in Section 2.5.

2.3 Macroscopic Stochastic Geometry Analysis

As discussed before, the spatial point process $\Pi = \mathit{\Pi}$ overviews the macroscopic-scale aspects of the network while the link queueing model delves into the microscopic-scale aspects of each transmitter-receiver pair. As shown in Fig. 2.1, queue arrivals, which represent the traffic generation at the transmitter, along with queue departures, which represent the successful packet reception at the receiver, allow the abstraction of the MWN to a network of spatially interacting queues. Due to the employed fixed rate transmission, a packet departure occurs if and only if the SINR at the intended receiver is greater that θ. As shown in Fig 2.2, the departure probabilities at different queues are not equivalent due to the location-dependent performance.

The first step to analyze the received SINR, and hence the queues departure probabilities, is to mark the point process of the transmitters by their activity parameters as $\Pi = \{\mathsf{y}_j, \mathsf{a}_j, \boldsymbol{\rho}_j\}$ where, for all $j \in \mathbb{N}^+$, the RVs a_j are i.i.d. Bernoulli marks with probability $\breve{p}_{\mathrm{a}} = \frac{p_{\mathrm{a}}}{N_{\mathrm{c}}}$, which is the probability that a link operates on any of the N_{c} channels due to the adopted F-ALOHA channel access, and $\boldsymbol{\rho}_j \in \mathcal{P} \cup \{0\}$ are non-negative, real-valued, and discrete marks of the node physical states. Due to the random channel selection and independent ALOHA transmission backoff, the marks a_j, $\forall j$, are independent. In contrast, the marks $\boldsymbol{\rho}_j$ are spatially and temporally correlated due to the static network topology that leads to location-dependent SINRs. As shown in Fig. 2.2, nodes at sparse locations are more likely to have successful transmissions and, hence, to empty their queues and are less likely to explore all power levels. On the other hand, nodes at congested locations are more likely to have transmission failures and, hence, to accumulate packets in their queues thus exploring all power levels. Such a spatiotemporal dependence of the protocol states complicates the analysis. Hence, we introduce the following approximation:

Approximation 1 (Power marks i.i.d. distribution) *We consider the marks $\boldsymbol{\rho}_j$ for all j to be i.i.d. from one node to another and from one time slot to another according to the spatially averaged steady-state distribution $\boldsymbol{w}_{\boldsymbol{\rho}} = [w^{[0]}, w^{[1]}, \ldots, w^{[N_{\mathrm{P}}]}]$.*

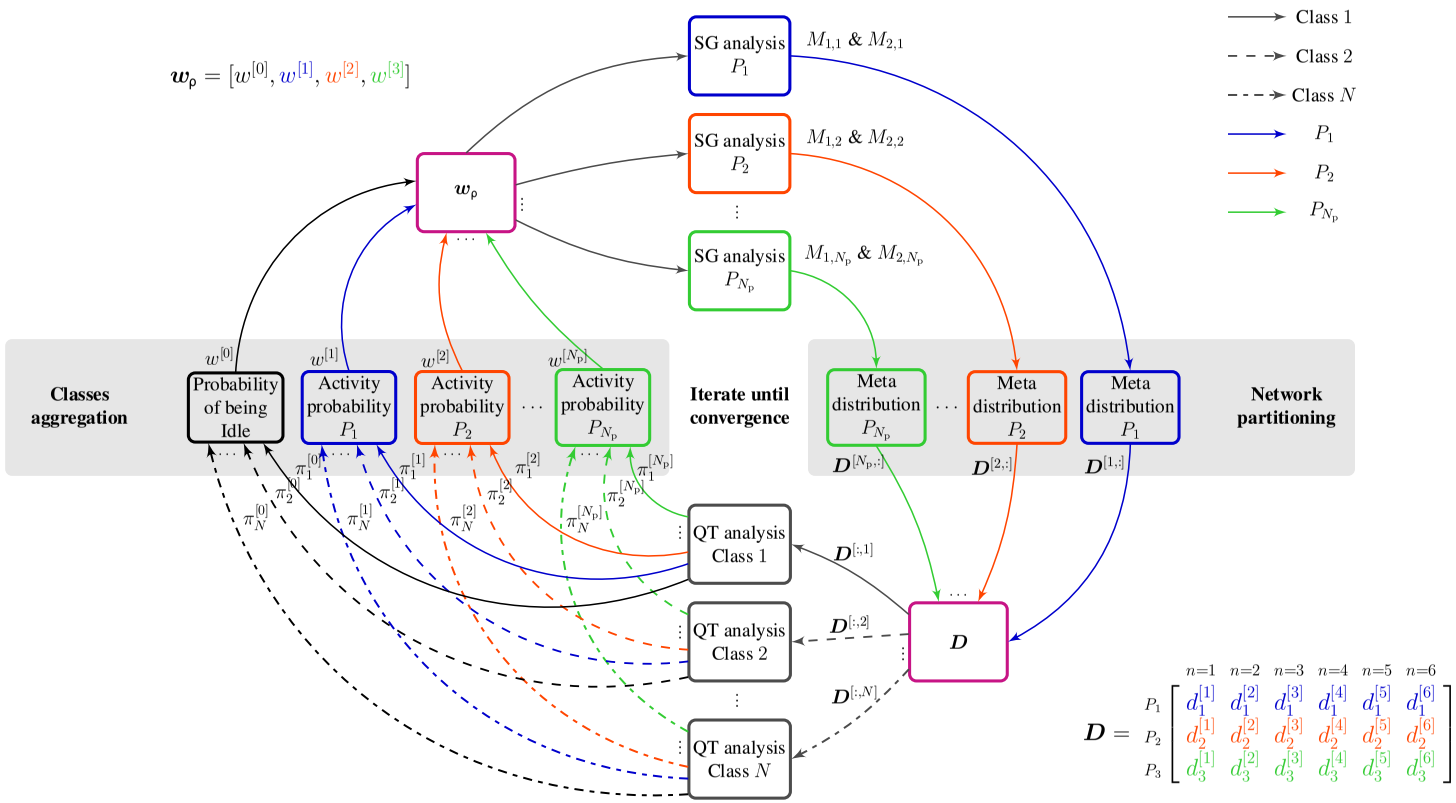

Figure 2.3: Methodology of analysis and iterative algorithm within the proposed spatiotemporal model.

The spatially averaged steady-state distribution $\boldsymbol{w}_{\mathsf{p}}$ is obtained in Section 2.4 via queueing theory by averaging over all possible location-dependent distributions of the node states. Note that Approximation 1 ignores the spatiotemporal correlations among the physical state marks of the interfering nodes on the aggregate interference and assumes identical distributions, which is mandatory for tractability[5] and is validated in Section 2.6. Thus, the goal of this section is to characterize the distribution of the transmission success probabilities (i.e., the meta distribution of the SINR) of the spatially interacting queues for i.i.d. exponentially distributed channel gains, i.i.d. access marks with uniform probability $\breve{p}_{\mathrm{a}}$, and i.i.d. node physical states marks with distribution $\boldsymbol{w}_{\mathsf{p}}$, where the interaction is due to the mutual interference between the links.

2.3.1 Meta Distribution Analysis

Let $\boldsymbol{y}_i \in \mathit{\Pi}$ and $\boldsymbol{y}_i^{\mathrm{rx}}$ be the location of a transmitter and its intended receiver. The SINR at the intended receiver can be characterized in terms of the intended transmitter power and the marked PPP of interferers as

$$p_{n_{\mathrm{p}},i} \triangleq \mathbb{P}\{\mathsf{z}_{n_{\mathrm{p}},i} > \theta | \mathsf{\Pi} = \mathit{\Pi}\} \tag{2.1a}$$

$$= \mathbb{P}\left\{ \frac{P_{n_{\mathrm{p}}} \mathsf{h}_i R^{-2\eta}}{\sum\limits_{j\,:\,\boldsymbol{y}_j \in \mathit{\Pi} \setminus \boldsymbol{y}_i} \mathsf{p}_j \mathsf{a}_j \mathsf{h}_j \|\boldsymbol{y}_j - \boldsymbol{y}_i^{\mathrm{rx}}\|^{-2\eta} + \sigma^2} > \theta \middle| \mathit{\Pi} \right\} \tag{2.1b}$$

where h_i is the channel gain of the intended link and σ^2 is the zero-mean Gaussian noise power. Note that the relative locations of the interfering transmitters are fixed. However, the randomness in (2.1) is due to the temporal variation of fading, random channel selection, node activities, and transmission states. Due to the location-dependent interference seen by each receiver $\boldsymbol{y}_i^{\mathrm{rx}}$, $p_{n_{\mathrm{p}},i}$ along the network can be seen as realizations of the RV $\mathsf{p}_{n_{\mathrm{p}}}$, of which CDF $F_{\mathsf{p}_{n_{\mathrm{p}}}}(\phi)$, namely the meta distribution of the SINR [113], provides the fraction of the network having a success probability smaller than ϕ. Moreover, thanks to the ergodicity of the PPP, $\mathsf{p}_{n_{\mathrm{p}}}$ can be formally defined as the success probability at the typical point for an arbitrary yet fixed node configuration, i.e.,

$$\mathsf{p}_{n_{\mathrm{p}}} \triangleq \mathbb{P}\{\mathsf{z}_{\circ} > \theta | \mathsf{\Pi}\} \tag{2.2}$$

[5]Specifically, Approximation 1 simplifies the computation of moments of the meta distribution of the SINR in Appendix A.1, Eq. (A.1b) (c.f. stationary i.i.d. marked point process [143, Corollary 7.4]).

taking values for different realizations of the point process. Thus we introduce the meta distribution of the SINR by the CDF

$$F_{\mathsf{p}_{n_\mathrm{p}}}(\phi) = \mathbb{P}^{\circ}\{\mathsf{p}_{n_\mathrm{p}} < \phi\} \tag{2.3}$$

where $\mathbb{P}^{\circ}\{\cdot\}$ is the probability over all the point configurations having a link at the typical point.

According to [113] the PDF of $\mathsf{p}_{n_\mathrm{p}}$ can be accurately approximated by the beta distribution as

$$f_{\mathsf{p}_{n_\mathrm{p}}}(\phi) = \frac{\phi^{\frac{M_{1,n_\mathrm{p}}(\alpha+1)-1}{1-M_{1,n_\mathrm{p}}}}(1-\phi)^{\alpha-1}}{B\big(\frac{M_{1,n_\mathrm{p}}\alpha}{1-M_{1,n_\mathrm{p}}},\alpha\big)} \tag{2.4a}$$

$$\alpha = \frac{(M_{1,n_\mathrm{p}} - M_{2,n_\mathrm{p}})(1-M_{1,n_\mathrm{p}})}{M_{2,n_\mathrm{p}} - M_{1,n_\mathrm{p}}^2} \tag{2.4b}$$

where $B(\cdot,\cdot)$ is the complete beta function and the moments M_{1,n_p} and M_{2,n_p} are given in the following Theorem 1.

Theorem 1 *The b^{th} order moment of the transmission success probabilities $\mathsf{p}_{n_\mathrm{p}}$ over all receivers in an arbitrary, but fixed, realization of the PBN is given by*

$$M_{b,n_\mathrm{p}} \triangleq \mathbb{E}^{\circ}\{\mathsf{p}_{n_\mathrm{p}}^b\} = e^{-b\theta_{n_\mathrm{p}}\sigma^2}\exp\{-\lambda\nu_{b,n_\mathrm{p}}\} \tag{2.5a}$$

$$\nu_{b,n_\mathrm{p}} = \pi\frac{1}{\eta}\sum_{k=1}^{b}\binom{b}{k}(-1)^{k+1} \cdot \int_0^{\infty}\left(\breve{p}_\mathrm{a}\sum_{i=1}^{N_\mathrm{p}}\frac{w^{[i]}\theta_{n_\mathrm{p},i}}{u+\theta_{n_\mathrm{p},i}}\right)^k u^{\frac{1-\eta}{\eta}}du \tag{2.5b}$$

where $\theta_{n_\mathrm{p}} = \theta R^{2\eta}/P_{n_\mathrm{p}}$, $\theta_{n_\mathrm{p},i} = \theta_{n_\mathrm{p}}P_i$, and $w^{[i]}$ is the i^{th} element in $\boldsymbol{w}_\mathsf{p}$. In case of $b=1$ the integral expression in (2.5b) *reduces to the following closed form*

$$\nu_{1,n_\mathrm{p}} = \pi\Gamma(1-\tfrac{1}{\eta})\Gamma(1+\tfrac{1}{\eta})\Big(\frac{\theta}{P_{n_\mathrm{p}}}\Big)^{\frac{1}{\eta}}R^2\breve{p}_\mathrm{a}\sum_{i=1}^{N_\mathrm{p}}w^{[i]}P_i^{\frac{1}{\eta}}. \tag{2.6}$$

Proof 1 *See Appendix A.1.*

Algorithm 1 Network partitioning in QoS-classes (meta distribution discretization).

Require: N, $\mathcal{P}$, λ, η, σ^2, θ.

Ensure: A departure probability vector $\boldsymbol{d}_{n_\mathrm{p}}$ s.t. $F_{\mathsf{p}_{n_\mathrm{p}}}(d_{n_\mathrm{p}}^{[n]}) - F_{\mathsf{p}_{n_\mathrm{p}}}(d_{n_\mathrm{p}}^{[n+1]}) = 1/N$ for all $n_\mathrm{p} \in \mathcal{N}_\mathrm{p}$ and $n \in \mathcal{N} \setminus \{N\}$.

for $n_\mathrm{p} = 1, 2, \ldots, N_\mathrm{p}$ **do**
  Compute the moments M_{1,n_p} and M_{2,n_p} through equation (2.5);
  Find $f_{\mathsf{p}_{n_\mathrm{p}}}(\phi)$ through equation (2.4);
  Set $\phi_1 = 0$ and $\phi_{N+1} = 1$;
  for $n = 1, 2, \ldots, N-1$ **do**
    Retrieve the values of ϕ_n and ϕ_{n+1} s.t.

$$F_{\mathsf{p}_{n_\mathrm{p}}}(\phi_n) - F_{\mathsf{p}_{n_\mathrm{p}}}(\phi_{n+1}) = \int_{\phi_n}^{\phi_{n+1}} f_{\mathsf{p}_{n_\mathrm{p}}}(\phi) d\phi = \frac{1}{N}$$

    Compute $d_{n_\mathrm{p}}^{[n]}$ s.t.

$$\int_{\phi_n}^{d_{n_\mathrm{p}}^{[n]}} f_{\mathsf{p}_{n_\mathrm{p}}}(\phi) d\phi = \int_{d_{n_\mathrm{p}}^{[n]}}^{\phi_{n+1}} f_{\mathsf{p}_{n_\mathrm{p}}}(\phi) d\phi = \frac{1}{2N};$$

  end for
  Assign $\boldsymbol{D}^{[n_\mathrm{p},:]} = \boldsymbol{d}_{n_\mathrm{p}}$;
end for
Return $\boldsymbol{D}$.

2.3.2 Network Uniform Partitioning

Consider that the PBN links are divided into different QoS-classes according to their location-dependent transmission success probabilities (or equivalently queue departure probabilities). If each possible value of $\mathsf{p}_{n_\mathrm{p}}$ is considered as a departure probability, then, an infinite number of QoS-classes are required to characterize the location-dependent performance of the nodes. For tractability, we resort to the following approximation.

Approximation 2 (Network uniform partitioning) *We partition the nodes into N equiprobable QoS-classes according to their transmission success probabilities. This is done by discretizing the continuous RV $\mathsf{p}_{n_\mathrm{p}}$ via a discrete*

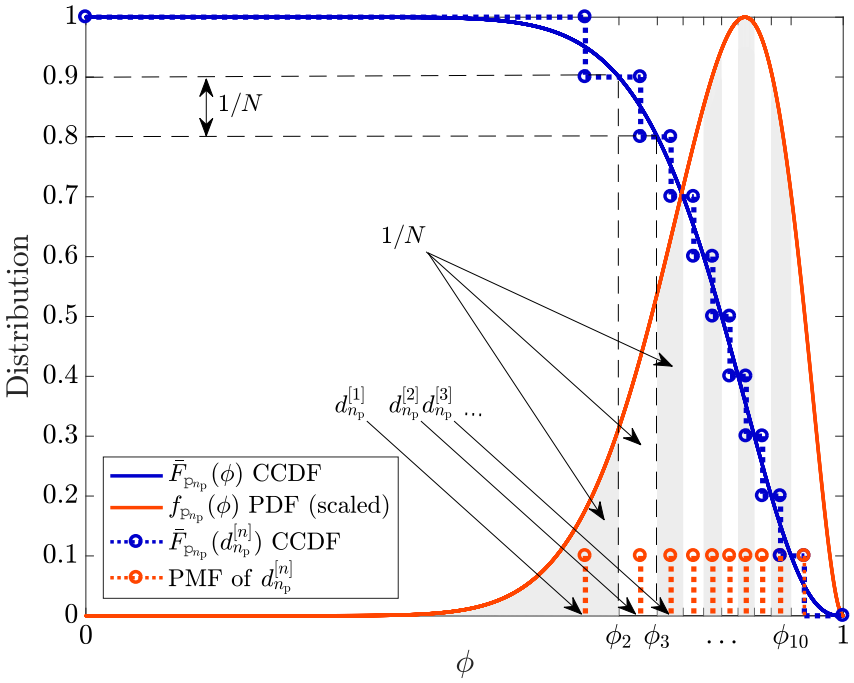

Figure 2.4: Distribution of the continuous conditional success probability and its discretization by importance sampling ($N = 10$).

RV $\mathsf{d}_{n_\mathrm{p}} \in \boldsymbol{d}_{n_\mathrm{p}}$. *The elements of* $\boldsymbol{d}_{n_\mathrm{p}} = [d_{n_\mathrm{p}}^{[1]}, d_{n_\mathrm{p}}^{[2]}, \ldots, d_{n_\mathrm{p}}^{[N]}]$ *are selected via the importance sampling criterion given in Algorithm 1, and illustrated in Fig. 2.4, such that the probabilities* $\mathbb{P}\{\mathsf{d}_{n_\mathrm{p}} = d_{n_\mathrm{p}}^{[n]}\} = 1/N$ *for all* $n \in \mathcal{N}$. *The process is repeated for all* $n_\mathrm{p} \in \mathcal{N}_\mathrm{p}$ *and the number of classes is selected to achieve a sufficiently accurate mathematical model.*

As shown in Algorithm 1, the matrix $\boldsymbol{D}$, of size $N_\mathrm{p} \times N$, can be populated using the discretized departure probability vectors $\boldsymbol{d}_{n_\mathrm{p}}$ for each power level. The element $\boldsymbol{D}^{[i,j]} = d_i^{[j]}$ defines the departure probability of the queue representing a link of the j^{th} QoS class when the intended transmitter operates with power level P_i. As shown in Fig. 2.3, the success probabilities' matrix $\boldsymbol{D}$ represents the interface from stochastic geometry analysis to queueing theory analysis. An example of the network partitioning proposed in Approximation 2 is illustrated in Fig. 2.2 for a single power level, i.e., $N_\mathrm{p} = 1$, and $N = 3$ QoS-classes. Since only a single power level is considered, success probabilities are given in the 1×3 vector $\boldsymbol{d} \in \{d^{[1]} = 0.56, d^{[2]} = 0.71, d^{[3]} = 0.84\}$, such that each value represents $1/3$ of the PBN links.

2.4 Microscopic Queueing Theory Analysis

To address the microscopic-scale analysis, each wireless link of the PBN is modeled as a queuing system as in Fig. 2.1 and then abstracted to a DTMC that tracks the number of packets in the transmitter buffer, employed transmission power, and retransmission phase as in Fig. 2.5. As discussed in Section 2.3, and shown in Figs. 2.2 and 2.4, the static locations of the considered PBN lead to temporally correlated packet departure probabilities for each queue. To capture the location-dependent performance of each queue while avoiding queueing memory complications, we resort to the following approximation:

Approximation 3 (QoS aware but temporally independent departure rates) *Recall that $\boldsymbol{D}$ is the power-QoS-class success probability matrix obtained by sampling the meta distribution of the SINR in Algorithm 1. At a generic time slot, the departure probability of a packet from a queue that belongs to the n^{th} QoS-class and operates with power n_{p} is given by $p_{\text{a}}\boldsymbol{D}^{[n_{\text{p}},n]}$. A queue does not change its QoS-class over time. The departures from the same queue in two different time slots when operating with transmission powers n_{p} in the first time slot and n'_{p} in the second time slot are assumed to be independent with probabilities $p_{\text{a}}\boldsymbol{D}^{[n_{\text{p}},n]}$ and $p_{\text{a}}\boldsymbol{D}^{[n'_{\text{p}},n]}$, respectively.*

The QoS-aware and memoryless success probabilities given in Approximation 3 facilitate the queueing theory analysis while capturing the location-dependent performance of each queue. Based on this approximation, the queueing model for each link (c.f. Fig. 2.1) is represented via a Geo/Ph/1 DTMC with the QoS-class dependent state diagram shown in Fig. 2.5, where the packet departure probabilities are given by $p_{\text{a}}\boldsymbol{D}^{[:,n]}$. Each of the DTMCs captures the different phases that a queue belonging to a given QoS-class may experience until a packet departure. In Geo/Ph/1 queues, the departure phase type distribution is constructed via an absorbing Markov chain that accounts for all phases that a queue may experience until packet departure [147, Ch. 5.8]. To built the transition matrix of the considered Geo/Ph/1 DTMC, we first define the following $N_{\text{t}} \times N_{\text{t}}$ matrices,

$$\boldsymbol{H}_{n_{\text{p}},n}^{[i,j]} = \begin{cases} \bar{p}_A & \text{if } i = j \\ p_{\text{a}}\bar{\boldsymbol{D}}^{[n_{\text{p}},n]} & \text{if } j = i+1 \\ 0 & \text{otherwise} \end{cases} \tag{2.7a}$$

$$\boldsymbol{J}_{n_{\text{p}},n}^{[i,j]} = \begin{cases} p_{\text{a}}\bar{\boldsymbol{D}}^{[n_{\text{p}},n]} & \text{if } i = N_{\text{t}} \text{ and } j = 1 \\ 0 & \text{otherwise} \end{cases} \tag{2.7b}$$

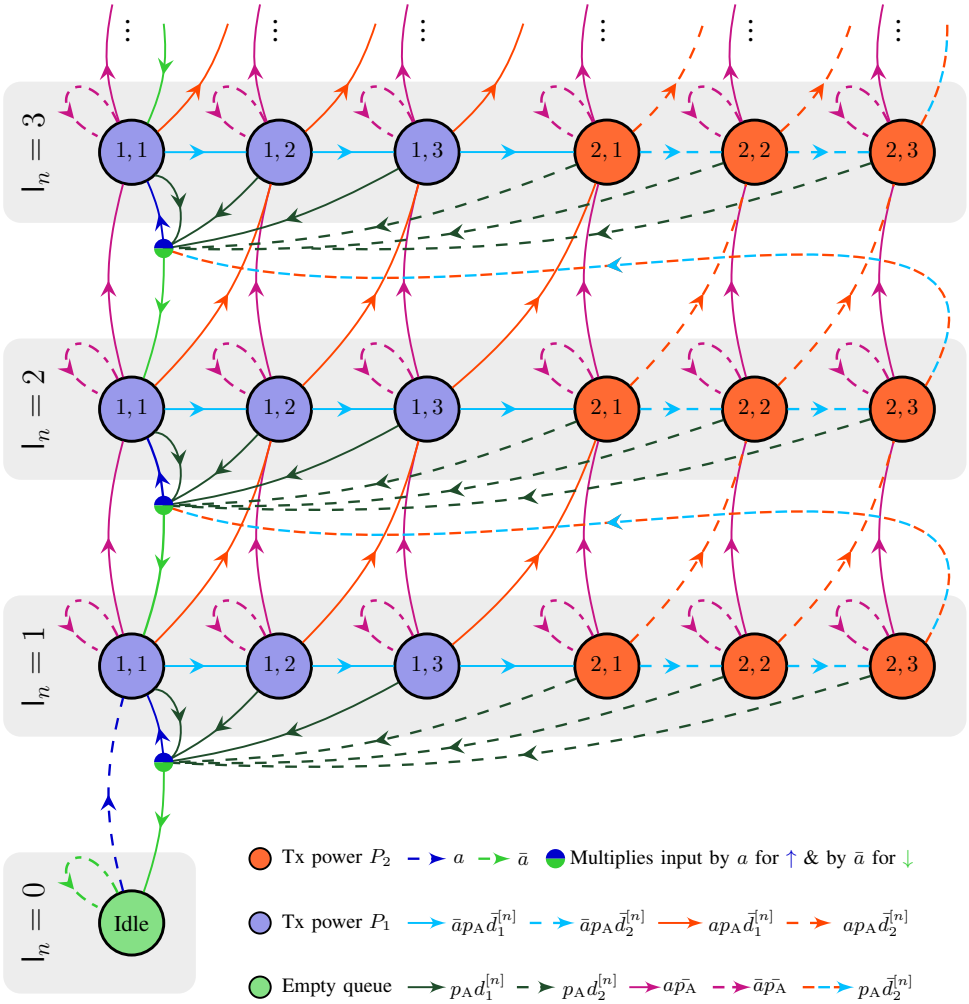

Figure 2.5: The DTMC for a class n queue with two power levels $\mathcal{P} = \{P_1, P_2\}$ and $N_{\mathrm{t}} = 3$ retransmissions per each power level.

where (2.7a) contains the probabilities of ALOHA deferral and horizontal transition between the logical phases (i.e., retransmissions counter value) within the same power level, and (2.7b) contains the probabilities of horizontal transition from one power level to the next. Given that there are N_{p} different power levels with N_{t} retransmissions within each power level, the transient state sub-stochastic matrix for the absorbing Markov chain is given by

$$\boldsymbol{S}_n = \begin{bmatrix} \boldsymbol{H}_{1,n} & \boldsymbol{J}_{1,n} & & & & \\ & \boldsymbol{H}_{2,n} & \boldsymbol{J}_{2,n} & & & \\ & & \ddots & \ddots & & \\ & & & \boldsymbol{H}_{N_\mathrm{p}-1,n} & \boldsymbol{J}_{N_\mathrm{p}-1,n} \\ \boldsymbol{J}_{N_\mathrm{p},n} & & & & \boldsymbol{H}_{N_\mathrm{p},n} \end{bmatrix}.^{6} \tag{2.8}$$

The $M \times M$ matrix $\boldsymbol{S}_n$, where $M = N_\mathrm{p} N_\mathrm{t}$, accounts for all powers and retransmissions phases until successful packet transmission (i.e., absorption). The absorption probabilities from each transient state phase is defined by the M-sized vector

$$\boldsymbol{s}_n = \mathbf{1} - \boldsymbol{S}_n \mathbf{1} = [s_n^{[1]}, s_n^{[2]}, \ldots, s_n^{[M]}]^\top, \tag{2.9a}$$

where $s_n^{[m]}$ is the probability that a packet is transmitted and is successfully decoded within a link of class n when the intended transmitter is in the phase $m = (n_\mathrm{p} - 1)N_\mathrm{t} + n_\mathrm{t}$. The index n_p of the transmission power used by the intended transmitter can be retrieved from m as $n_\mathrm{p} = \lceil m/N_\mathrm{t} \rceil$ and, hence, $s_n^{[m]} = p_\mathrm{a} d_{n_\mathrm{p}}^{[n]}$.[7] Since the transmission of each new packet starts with power $n_\mathrm{p} = 1$ and $n_\mathrm{t} = 1$, the initialization vector for the absorbing Markov chain is $\boldsymbol{\beta} = [1,\ 0,\ 0, \ldots, 0] \in \mathbb{R}^{M \times 1}$.

Using $\boldsymbol{S}_n$, $\boldsymbol{s}_n$, and $\boldsymbol{\beta}$, the DTMC modeling of the n^{th} QoS-class link is given by a quasi-birth-and-death (QBD) process with the following transition matrix

$$\boldsymbol{P}_n = \begin{array}{c} \\ \mathsf{l}_n{=}0 \\ \mathsf{l}_n{=}1 \\ \mathsf{l}_n{=}2 \\ \mathsf{l}_n{=}3 \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccccccc} \mathsf{l}_n{=}0 & \mathsf{l}_n{=}1 & \mathsf{l}_n{=}2 & \mathsf{l}_n{=}3 & \mathsf{l}_n{=}4 & \cdots \end{array} \\ \begin{bmatrix} \boldsymbol{B}_n & \boldsymbol{C}_n & & & & \\ \boldsymbol{E}_n & \boldsymbol{A}_{1,n} & \boldsymbol{A}_{0,n} & & & \\ & \boldsymbol{A}_{2,n} & \boldsymbol{A}_{1,n} & \boldsymbol{A}_{0,n} & & \\ & & \boldsymbol{A}_{2,n} & \boldsymbol{A}_{1,n} & \boldsymbol{A}_{0,n} & \\ & & & \ddots & \ddots & \ddots \end{bmatrix} \end{array} \tag{2.10}$$

where l_n represents the different levels (i.e., number of packets in the queue) within a generic n^{th} class queue, $\boldsymbol{B} = \bar{a} \in \mathbb{R}$, $\boldsymbol{E}_n = \bar{a}\boldsymbol{s}_n \in \mathbb{R}^{M \times 1}$, $\boldsymbol{C} = a\boldsymbol{\beta} \in \mathbb{R}^{1 \times M}$, $\boldsymbol{A}_{0,n} = a\boldsymbol{S}_n \in \mathbb{R}^{M \times M}$, $\boldsymbol{A}_{1,n} = a\boldsymbol{s}_n\boldsymbol{\beta} + \bar{a}\boldsymbol{S}_n \in \mathbb{R}^{M \times M}$, and $\boldsymbol{A}_{2,n} = \bar{a}\boldsymbol{s}_n\boldsymbol{\beta} \in \mathbb{R}^{M \times M}$. The steady-state distribution of a queue with transition

[6] In case of F-ALOHA with no power ramping, i.e., $M = N_\mathrm{p} = N_\mathrm{t} = 1$, the transient state sub-stochastic matrix is simply given by $\boldsymbol{S}_n = \boldsymbol{H}_n + \boldsymbol{J}_n$.

[7] The superscript m is used for brevity where the specification of n_p and n_t is not needed. In general a transmission phase is always associated with a single transmission power-retransmission index pair.

matrix $\boldsymbol{P}_n$ is obtained by solving the following system of equations

$$\boldsymbol{x}_n \boldsymbol{P}_n = \boldsymbol{x}_n \tag{2.11a}$$
$$\boldsymbol{x}_n \mathbf{1} = 1 \tag{2.11b}$$

where $\boldsymbol{x}_n = [x_n^{[0]}, \boldsymbol{x}_n^{[1]}, \boldsymbol{x}_n^{[2]}, \ldots, \boldsymbol{x}_n^{[l]}, \ldots]$ is the steady-state probability vector for all levels $l = 1, 2, \ldots$ of an n^{th} class' queue; $x_n^{[0]}$ is the idle-state probability; $\boldsymbol{x}_n^{[l]} = [x_{l,n}^{[1]}, x_{l,n}^{[2]}, \ldots, x_{l,n}^{[M]}]$ is the distribution of phases in level l, and $x_{l,n}^{[m]}$ is the probability of being at level l and phase $m = (n_{\text{p}} - 1)N_{\text{t}} + n_{\text{t}}$. As mentioned before, the transmission power index used in the phase m is $n_{\text{p}} = \lceil m/N_{\text{t}} \rceil$.

Since the considered queueing model is ergodic and irreducible, then the system of equations in (2.11) has a unique solution if the queue is stable. To check the stability, we first construct the matrix $\boldsymbol{A}_n = \boldsymbol{A}_{0,n} + \boldsymbol{A}_{1,n} + \boldsymbol{A}_{2,n} = \boldsymbol{s}_n \boldsymbol{\beta} + \boldsymbol{S}_n$, and solve the system

$$\boldsymbol{\psi}_n \boldsymbol{A}_n = \boldsymbol{\psi}_n \tag{2.12a}$$
$$\boldsymbol{\psi}_n \mathbf{1} = 1 \tag{2.12b}$$

for $\boldsymbol{\psi}_n = [\psi_n^{[1]}, \psi_n^{[2]}, \ldots, \psi_n^{[M]}]$, which is the marginal distribution of all transmission phases while excluding the idle state. Then, following [147], the queue is stable if and only if (i.f.f.)

$$\boldsymbol{\psi}_n \boldsymbol{A}_{2,n} \mathbf{1} > \boldsymbol{\psi}_n \boldsymbol{A}_{0,n} \mathbf{1}\,. \tag{2.13}$$

The output of the condition (2.13) leads to two different types of analysis, namely, stable and unstable class analysis.

2.4.1 Stable QoS-class analysis

If the condition in (2.13) is satisfied, then the QoS-class represented by (2.11) is stable and has a unique solution. Then, using the systematic matrix analytic method (MAM) [147], the system in (2.11) has the following solution

$$x_n^{[0]} = \left(1 + \boldsymbol{C}\left(\boldsymbol{I} - a\boldsymbol{s}_n\boldsymbol{\beta} - \bar{a}\boldsymbol{S}_n - \boldsymbol{R}_n\bar{a}\boldsymbol{s}_n\boldsymbol{\beta}\right)^{-1} \cdot (\boldsymbol{I} - \boldsymbol{R}_n)^{-1}\,\mathbf{1}\right)^{-1} \tag{2.14a}$$

$$\boldsymbol{x}_n^{[l]} = \begin{cases} x_n^{[0]}\boldsymbol{C}\left(\boldsymbol{I} - a\boldsymbol{s}_n\boldsymbol{\beta} - \bar{a}\boldsymbol{S}_n - \boldsymbol{R}_n\bar{a}\boldsymbol{s}_n\boldsymbol{\beta}\right)^{-1} & \text{for } \; l = 1 \\ \boldsymbol{x}_n^{[1]}\boldsymbol{R}_n^{l-1} & \text{for } \; l > 1 \end{cases} \tag{2.14b}$$

where $\boldsymbol{I} \in \mathbb{R}^{M\times M}$ is the identity matrix and $\boldsymbol{R}_n \in \mathbb{R}^{M\times M}$ is the MAM rate matrix given by

$$\boldsymbol{R}_n = a\boldsymbol{S}_n \left(\boldsymbol{I} - a\boldsymbol{s}_n\boldsymbol{\beta} - \bar{a}\boldsymbol{S}_n - a\boldsymbol{S}_n\mathbf{1}\boldsymbol{\beta}\right)^{-1}. \tag{2.15}$$

Let $\boldsymbol{\zeta}_n = [\zeta_n^{[1]}, \zeta_n^{[2]}, \ldots, \zeta_n^{[M]}]$ be the vector containing the probabilities of being in phase m irrespective of the buffer level, then

$$\boldsymbol{\zeta}_n = \boldsymbol{x}_n^{[1]} \left(\boldsymbol{I} - \boldsymbol{R}_n\right)^{-1}. \tag{2.16}$$

Note that $\boldsymbol{\zeta}_n$ is a sub-stochastic vector as it does not contain the probability of being idle. The steady-state marginal distribution for the powers levels $\boldsymbol{\pi}_n$ is given by

$$\pi_n^{[0]} = x_n^{[0]} \tag{2.17a}$$

$$\pi_n^{[n_\mathrm{p}]} = \sum_{m=1}^{M} \mathbb{1}_{\mathcal{M}}(m)\, \zeta_n^{[m]} \tag{2.17b}$$

where $\mathbb{1}_{\{\cdot\}}$ is the indicator function that equals one if $m \in \mathcal{M} = \{m' : \lceil m'/N_\mathrm{t} \rceil = n_\mathrm{p}\}$ and zero otherwise, which ensures that the sum is over the retransmission phases within the same transmission power index n_p.

2.4.2 Unstable QoS-class analysis

If the condition in (2.13) is not satisfied, then the QoS-class represented by (2.11) is unstable and the buffer will overflow with probability one. In this case, the probability of being idle is zero $x_n^{[0]} = 0$ and the marginal distribution of the phases is the one obtained from solving (2.12). Hence, the steady-state marginal distribution $\boldsymbol{\pi}_n$ for the power levels is given by

$$\pi_n^{[0]} = 0 \tag{2.18a}$$

$$\pi_n^{[n_\mathrm{p}]} = \sum_{m=1}^{M} \mathbb{1}_{\mathcal{M}}(m)\, \psi_n^{[m]}. \tag{2.18b}$$

2.4.3 Classes aggregation

As shown in Fig 2.3, the classes aggregation is the interface between queueing theory and stochastic geometry analysis, where the spatially averaged $\boldsymbol{w}_{\boldsymbol{\rho}}$ is obtained. As mentioned in Approximation 1, the spatial and temporal

correlations among the activity marks of the interfering nodes are ignored and the aggregate interference is characterized assuming i.i.d. node state distribution $\boldsymbol{w}_{\boldsymbol{\rho}}$. Recall that the network is partitioned into N equiprobable classes (c.f. Approximation 2), the spatially averaged node state distribution is defined for $i = 0, 1, \ldots, N_{\mathrm{p}}$ by

$$w^{[i]} = \frac{1}{N} \sum_{n=1}^{N} \pi_n^{[i]} \,. \tag{2.19}$$

2.5 Spatiotemporal Model Solution

As shown in Section 2.3, the characterization of the meta distribution of the SINR and the subsequent packet success probabilities matrix $\boldsymbol{D}$ require the spatially averaged node state distribution $\boldsymbol{w}_{\boldsymbol{\rho}}$. Meanwhile, computing $\boldsymbol{w}_{\boldsymbol{\rho}}$ through queueing theory in Section 2.4 requires the packet departure probability matrix $p_{\mathrm{a}}\boldsymbol{D}$, which is obtained by sampling the meta distribution of the SINR. To solve the coupling between $\boldsymbol{D}$ and $\boldsymbol{w}_{\boldsymbol{\rho}}$, we follow the iterative algorithm shown in Fig. 2.3 and detailed in Algorithm 2. Note that the system to be solved, i.e.,

$$\boldsymbol{x}_n^{[k]} \boldsymbol{P}_{\boldsymbol{n}}(\boldsymbol{x}_n^{[k-1]}) = \boldsymbol{x}_n^{[k]} \tag{2.20a}$$

$$\boldsymbol{x}_n^{[k]} \mathbf{1} = 1 \tag{2.20b}$$

is known to converge according to the fixed-point theorem [122,137,148,149].

2.5.1 Network Stability

According to the Loynes theorem [150], a stable queue is the one that have the packet departure probability greater than the packet arrival probability, which guarantees finite average buffer size and bounded queueing delay. Otherwise, the buffer overflows with probability one and the queueing delay becomes unbounded. Recalling the stability condition in (2.13), the fraction of nodes that operate with stable queues can be obtained as

$$\gamma_{\mathrm{su}} = \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\mathcal{S}}(n) \tag{2.21}$$

where $\mathcal{S} = \{n' : \boldsymbol{\psi}_{n'} \boldsymbol{A}_{2,n'} \mathbf{1} > \boldsymbol{\psi}_{n'} \boldsymbol{A}_{0,n'} \mathbf{1}\}$; and $\boldsymbol{\psi}_n$, $\boldsymbol{A}_{2,n}$, and $\boldsymbol{A}_{0,n}$ are obtained from Algorithm 2 for every QoS-class after convergence. Now consider the multidimensional space of the system parameters with points defined as

Algorithm 2 Iterative algorithm with N activity classes for networks of Geo/Ph/1 queues

Require: λ, p_{a}, a, N, θ, η, R, σ^2, N_{c}, N_{p}, N_{t}, $\mathcal{P}$.
Ensure: $\boldsymbol{D}$ and for all $n \in \mathcal{N}$, $\boldsymbol{x}_n$ for stable classes and $\boldsymbol{\psi}_n$ for unstable classes.

Inizialize $k = 1$, $\epsilon \ll 1$, $\boldsymbol{w}_{\mathsf{p}}^{[1]}$ s.t. $\boldsymbol{w}_{\mathsf{p}}^{[1]}\mathbf{1} = 1$.
while $\max_n \{ \|\boldsymbol{w}_{\mathsf{p}}^{[k]} - \boldsymbol{w}_{\mathsf{p}}^{[k-1]}\| \} \geq \epsilon$ **do**
  for $n_{\mathrm{p}} \in \mathcal{P}$ **do**
    Compute the moments $M_{1,n_{\mathrm{p}}}$ and $M_{2,n_{\mathrm{p}}}$ through equation (2.5);
    Run Algorithm 1 to populate $\boldsymbol{D}$;
  end for
  for $n \in \mathcal{N}$ **do**
    Construct the matrix $\boldsymbol{S}_n$ and the vector $\boldsymbol{s}_n$ according to (2.7a), (2.7b), (2.8), and (2.9);
    Construct $\boldsymbol{A}_n = \boldsymbol{A}_{0,n} + \boldsymbol{A}_{1,n} + \boldsymbol{A}_{2,n}$ and solve (2.12) for $\boldsymbol{\psi}_n$;
    if $\boldsymbol{\psi}_n \boldsymbol{A}_{2,n}\mathbf{1} > \boldsymbol{\psi}_n \boldsymbol{A}_{0,n}\mathbf{1}$ **then**
      the queues belonging tho the n^{th} class are stable;
      Obtain $\boldsymbol{x}_n$ through (2.14);
      Evaluate $\boldsymbol{\pi}_n$ through (2.16) and (2.17)
    else
      the n^{th} class is unstable. Set $\pi_n^{[0]} = 0$ and retrieve $\boldsymbol{\psi}_n$ to find $\boldsymbol{\pi}_n$ via (2.18);
    end if
  end for
  Use $\boldsymbol{\pi}_n$ for all classes to calculate $\boldsymbol{w}_{\mathsf{p}}^{[k+1]}$ through (2.19);
end while
Return $\boldsymbol{x}_n$ for stable classes, $\boldsymbol{\psi}_n$ for non-stable classes, $M_{1,n_{\mathrm{p}}}$, $M_{2,n_{\mathrm{p}}}$, and $\boldsymbol{D}$.

$\mathcal{R} = \{\lambda, \theta, a, p_{\mathrm{a}}\} \in \mathcal{G} = [\mathbb{R}^+]^2 \times [0,1]^2$. Consider the function $\gamma_{\mathrm{su}} : \mathcal{G} \to [0,1]$, we define the *$\gamma$-stability region* as

$$\mathcal{R}_\gamma^{\mathrm{s}} \triangleq \{\mathcal{R} \,:\, \gamma_{\mathrm{su}}(\mathcal{R}) > \gamma\} \tag{2.22}$$

i.e., as the region where a fraction of the nodes greater than γ operates with stable queues. In addition to the de facto stability condition in (2.21), necessary (NC) and sufficient (SC) conditions for the γ-stability of the PBN can be checked through the mildest and most severe interference scenarios, respectively. Note that the NC and SC do not require an iterative algorithm and can be directly determined. In particular, the NC can be obtained by setting $\boldsymbol{w}_{\mathsf{p}} = \boldsymbol{w}_{\mathsf{p}}^{\mathrm{nc}} = [1-a, 0, \ldots, 0, a]$, which captures the mildest interference

scenario by activating the nodes with fresh packets only. In contrast, SC can be obtained by setting $\boldsymbol{w}_{\mathsf{p}} = \boldsymbol{w}_{\mathsf{p}}^{\mathrm{sc}} = [0, 1, 0, \ldots, 0]$, which captures the most sever interference scenario by activating all nodes.[8] This would lead to explicit expressions for the success probability moments as shown in the following corollary

Corollary 1 *Assuming interference limited regime, the b^{th} order moment of the transmission success probabilities in the mildest and most severe interference scenarios are, respectively, given by*

$$M_b^{\mathrm{nc}} = \exp\left\{ -\frac{\pi\lambda}{\eta} \sum_{k=1}^{b} \binom{b}{k} \int_0^{\infty} \left(\frac{a\breve{p}_{\mathrm{a}} \theta R^{2\eta}}{u + \theta R^{2\eta}} \right)^k \frac{(-1)^{k+1}}{u^{\frac{\eta-1}{\eta}}} du \right\} \tag{2.23a}$$

$$M_b^{\mathrm{sc}} = \exp\left\{ -\frac{\pi\lambda}{\eta} \sum_{k=1}^{b} \binom{b}{k} \int_0^{\infty} \left(\frac{\breve{p}_{\mathrm{a}} \theta R^{2\eta}}{u + \theta R^{2\eta}} \right)^k \frac{(-1)^{k+1}}{u^{\frac{\eta-1}{\eta}}} du \right\}. \tag{2.23b}$$

Proof 2 *Follows directly from Theorem 1 by ignoring noise, assuming that all active transmitters operate with equal powers, and setting $\boldsymbol{w}_{\mathsf{p}} = \boldsymbol{w}_{\mathsf{p}}^{\mathrm{nc}}$ and $\boldsymbol{w}_{\mathsf{p}} = \boldsymbol{w}_{\mathsf{p}}^{\mathrm{sc}}$.* □

The percentile of the PBN satisfying the NC can be checked using Algorithm 3. The same algorithm can be also used to check the percentile of the PBN satisfying the SC by replacing M_b^{nc} with M_b^{su}.

2.5.2 Performance Metrics

Once the steady-state probabilities (i.e., $\boldsymbol{x}_n$ and $\boldsymbol{\psi}_n$), the moments of the SINR (i.e., $M_{1,n_{\mathrm{p}}}$ and $M_{2,n_{\mathrm{p}}}$), and the success probability matrix $\boldsymbol{D}$ are determined by Algorithm 2, many performance metrics can be computed. For instance, following [147, Ch. 5.8] for Geo/Ph/1 queues, the *average queue length* of a node that belongs to the n^{th} QoS-class is given by

$$\mathbb{E}\left\{\mathsf{l}_n\right\} = \boldsymbol{x}_n^{[1]} (\boldsymbol{I} - \boldsymbol{R})^{-2} \mathbf{1} \tag{2.24}$$

Let t_{q} denote the queueing delay, i.e., the number of time slots a packet spends in the queue before the transmission starts. Following [147, Ch. 5.8.1], the *average queuing delay* in the n^{th} class is given by

$$\mathbb{E}\left\{\mathsf{t}_{\mathrm{q},n}\right\} = \sum_{t=1}^{\infty} t\, \mathbb{P}\left\{\mathsf{t}_{\mathrm{q},n} = t\right\} \tag{2.25}$$

[8] Since ramping-up and ramping-down protocols use a single power in case of severe or mild interference scenario we just define $\boldsymbol{w}_{\mathsf{p}}^{\mathrm{nc}}$ and $\boldsymbol{w}_{\mathsf{p}}^{\mathrm{sc}}$ for the ramping-down protocol.

Algorithm 3 NC for Percentile Stability

Require: M_b^{nc}, a, N, N_{c}, N_{p}, N_{t}.
Ensure: γ

Inizialize $i = 0$.
Obtain $\boldsymbol{d}$ via Algorithm 1;
for $n \in \mathcal{N}$ **do**
    Construct $\boldsymbol{S}_n$ and $\boldsymbol{s}_n$ according to (2.7a), (2.7b), (2.8), and (2.9);
    Construct $\boldsymbol{A}_n = \boldsymbol{A}_{0,n} + \boldsymbol{A}_{1,n} + \boldsymbol{A}_{2,n}$ to solve (2.12) for $\boldsymbol{\psi}_n$;
    if $\boldsymbol{\psi}_n \boldsymbol{A}_{2,n} \mathbf{1} > \boldsymbol{\psi}_n \boldsymbol{A}_{0,n} \mathbf{1}$ **then**
        $i = i + 1$;
    else
        Break;
    end if
end for
Return The NC is satisfied for $\gamma = \frac{i}{N}\%$ of the PBN.

The distribution of the queuing delay can be evaluated by solving the queuing problem of an absorbing DTMC that tracks the position of a target packet in the queue. In particular, define the queue distribution at time t as $\boldsymbol{\delta}_n^{[t]} = \left[\delta_{n,t}^{[0]}, \boldsymbol{\delta}_{n,t}^{[1]}, \boldsymbol{\delta}_{n,t}^{[2]}, \dots\right]$ where $\boldsymbol{\delta}_{n,t}^{[l]} = \left[\delta_{l,n,t}^{[1]}, \delta_{l,n,t}^{[2]}, \dots, \delta_{l,n,t}^{[M]}\right]$; $\boldsymbol{x}_n$ gives the state probability of the system upon a packet arrival, i.e. $\boldsymbol{\delta}_n^{[0]} = \boldsymbol{x}_n$; and the absorption occurs when the tagged packet arrives at the queue head. The transition matrix s.t. $\left(\boldsymbol{\delta}_n^{[t]}\right)^\top = \left(\boldsymbol{\delta}_n^{[t-1]}\right)^\top \boldsymbol{P}_{\mathsf{t}_{\mathrm{q},n}}$ is as follows

$$\boldsymbol{P}_{\mathsf{t}_{\mathrm{q},n}} = \begin{bmatrix} \mathbf{1} & & & & \\ \boldsymbol{s}_n & \boldsymbol{S}_n & & & \\ & \boldsymbol{s}_n\boldsymbol{\beta} & \boldsymbol{S}_n & & \\ & & \boldsymbol{s}_n\boldsymbol{\beta} & \boldsymbol{S}_n & \\ & & & \ddots & \ddots \end{bmatrix}. \tag{2.26}$$

By following this interpretation, the queuing delay distribution is given by

$$\mathbb{P}\left\{\mathsf{t}_{\mathrm{q},n} \leq t\right\} = \delta_{n,t}^{[0]}. \tag{2.27}$$

When the packet is at head of the queue, it will take additional t_{s} time slots to be successfully delivered to the receiver over the wireless channel. Note that the service delay t_{s} accounts for both ALOHA transmission deferrals and transmissions failures due to the SINR being less than θ. The *average service delay* for a node belonging to the n^{th} QoS-class is given by

$$\mathbb{E}\left\{\mathsf{t}_{\mathrm{s},n}\right\} = \sum_{i=1}^{N_{\mathrm{p}}} \frac{\pi_n^{[i]}}{1 - x_n^{[0]}} \frac{1}{p_{\mathrm{a}} D^{[i,n]}} \tag{2.28}$$

Let t_n be the total, i.e., queuing plus service, delay from arrival until reception. Then, the average total delay is given by

$$\mathbb{E}\left\{\mathsf{t}_n\right\} = \mathbb{E}\left\{\mathsf{t}_{\mathrm{q},n}\right\} + \mathbb{E}\left\{\mathsf{t}_{\mathrm{s},n}\right\} . \tag{2.29}$$

It is worth noting that the average queuing delay for unstable queues is infinite. However, the average service delay is finite and is given by (2.28).

An important concept that we introduce in this paper is the γ-*operativity*. Analogously to the definition in (2.22), we define the γ-*operativity* region by the function $\gamma_{\mathrm{to}} : \mathcal{G} \to [0, 1]$ as

$$\mathcal{R}_\gamma^{\mathrm{o}} \triangleq \{\mathcal{R} \,:\, \gamma_{\mathrm{to}}(\mathcal{R}) > \gamma\} \tag{2.30}$$

which determines the region of the points in the space of network parameters that satisfy a target performance (e.g., delay, queue length, etc.). The parameter γ_{to} defines the fraction of nodes that achieves the target operation. For example, when the target operation is defined in terms of maximum tolerable delay $t^\star$ the γ-*operativity* is given by

$$\gamma_{\mathrm{to}} = \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\mathcal{T}}(n) \tag{2.31}$$

where $\mathcal{T} = \{n' : \mathbb{E}\left\{\mathsf{t}_{n'}\right\} \leq t^\star\}$.

2.6 Numerical Results and Discussion

We start by validating the developed spatiotemporal model, particularly Approximations 1-3, via independent Montecarlo simulations. The simulation is conducted over an arbitrary, but fixed, realization of the PBN in a 10×10 km^2 area with a wrapped-around boundaries.[9] Only the fading realizations and node activities change over the temporal domain. Each simulation run is considered as a time slot where independent channel gains are realized, packets are generated, and nodes interact according to their protocol states and relative positions. We keep track of the queue level, transmission power,

[9]Wrap-around simulation model is utilized to eliminate edge-induced favorable interference conditions and their subsequent effects on queueing departure probabilities.

and retransmission phase of each queue. For a transition from one time slot to another, packets are independently generated in all buffers with probability a. A transmitter with non-empty buffer becomes active with probability p_{a} and uniformly selects one of the N_{c} channels. The SINRs at the receivers of all active links are determined based on the interferers that are simultaneously active on the same channel. Then, one packet is subtracted only from queues of the links with SINR greater than θ. The simulation starts from a fictitious point in time where all nodes are considered idle and then runs for a sufficiently high number of time slots until the steady-state is reached. Let $\widehat{\boldsymbol{w}}_{\boldsymbol{\rho}}^{[k]}$ be the distribution of nodes activity at the k^{th} simulation run, then steady-state is reached when $\max \|\widehat{\boldsymbol{w}}_{\boldsymbol{\rho}}^{[k]} - \widehat{\boldsymbol{w}}_{\boldsymbol{\rho}}^{[k-1]}\| < \epsilon$. The time slot at which steady-state is reached is the starting point of the simulation kernel where all temporal statistics are computed. For the simulations, we choose $\epsilon = 10^{-3}$ and use a kernel of 10,000 iterations. Throughout the considered simulation kernel, the SINRs of the receivers of all active links along with the transmission powers of their intended transmitters are recoded to construct the meta distribution of the success probability for all transmission power levels.

Figs. 2.6 and 2.7 show the meta distributions of the transmission success probability for different nodes intensities, ALOHA access probabilities, and transmission rates. Particularly, Fig. 2.6 is plotted for a single power level ALOHA protocol and Fig. 2.7 is plotted for a power-ramping ALOHA protocol with two power levels. In both figures, the analysis curves are plotted via (2.4) and the moments are obtained from Algorithm 2 after convergence. Both figures show perfect match between the theoretical (solid lines) and simulation (markers) results as long as sufficiently high number of QoS-classes (i.e., $N = 10$) are considered, thus validating the considered model. The figures also show the significance of the system parameters, such as transmission rates, medium access probability, and transmission rates, on the distribution of the success probability.

Fig. 2.8 shows the average queuing length as a function of the node density for the first ($n = 1$, red diamonds) and last ($n = 10$, green stars) QoS-classes as well as the spatially averaged queue length. Although an infinite queue size is assumed in the analysis, the figure shows that a finite queue with reasonable buffer size is required as long as the node operates within a stable QoS-class. If the queue is unstable, the buffer will overflow with probability one regardless of the buffer size. It is worth noting that the curve of the high class $N = 10$ experience a discontinuity (i.e., jump) at the point where a lower class becomes unstable. Such discontinuity occur because the entire nodes within the unstable class (i.e., $1/N$ fraction of the total nodes) becomes active all the time and contribute to the aggregate interference.

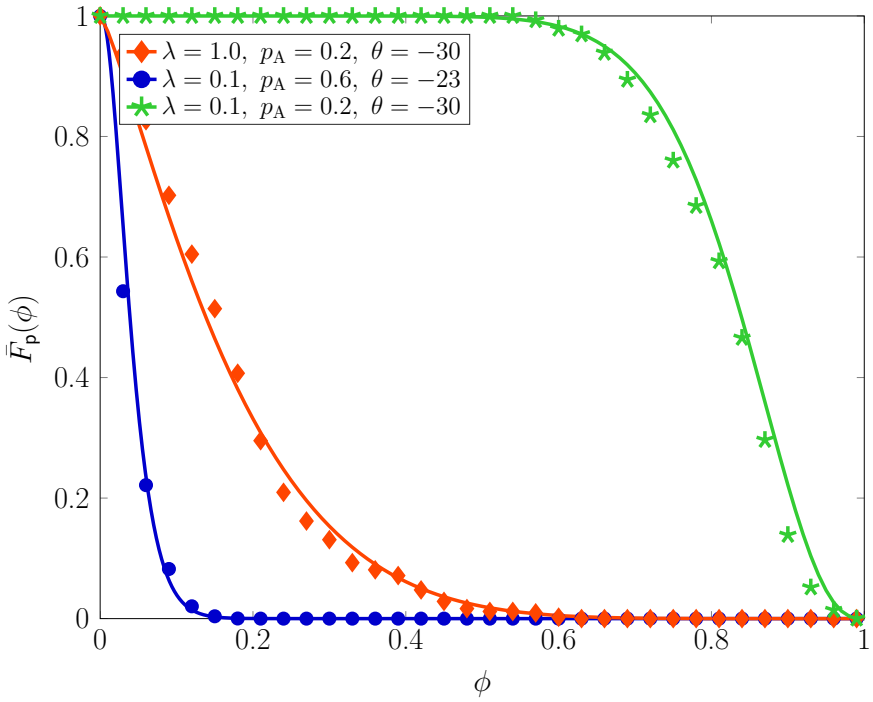

Figure 2.6: CCDFs of p in different network scenarios for simple ALOHA ($N_{\mathrm{p}} = 1$). Theoretical values are shown for $N = 10$ (solid lines) along with simulated values (markers) for $\eta = 2$, $R = 10$ [m], $\sigma^2 = -90$ [dBm], $\mathcal{P} = \{-30\}$ [dBm], $a = 0.1$ [packets/slots].

Figs 2.9-2.12 show the Pareto frontier for the system parameters that ensure a stable queue operation for a γ fraction of the nodes. Each of the colored region show the pairs of the network parameters that are required to ensure stability for a given faction of nodes. The color mapping to the network fraction γ is shown in the bars located on the right of each figure. The magenta dashed line with markers, denoted as *deterministic stability frontier* shows the region of the network parameters that are required to ensure network stability on average,[10] i.e.,

$$\mathcal{R}^{\mathrm{s}}_{\mathrm{av}} \triangleq \{\mathcal{R} : p_{\mathrm{a}} M_1(\mathcal{R}) > a\} \tag{2.32}$$

which conveys no information about the fraction of nodes that may have

[10]Such a region is determined through the classic spatially averaged success probability. For simplicity, in the case of (2.32) we show the condition for single phase, i.e., Geo/Geo/1 queues.

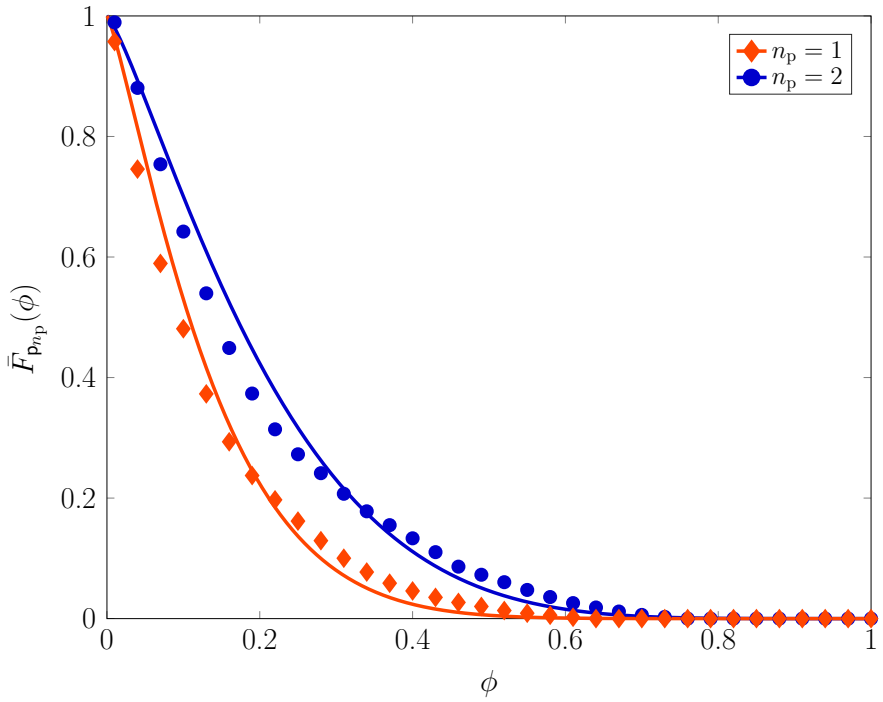

Figure 2.7: CCDFs of $\mathsf{p}_{n_\mathrm{p}}$ for aloha with power-ramping. Theoretical values are shown for $N = 10$ (solid lines) along with simulated (markers) values for $\lambda = 0.1$, $\eta = 2$, $R = 10$ [m], $\sigma^2 = -90$ [dBm], $N_\mathrm{c} = 1$, $N_\mathrm{p} = 2$, $N_\mathrm{t} = 2$, $\mathcal{P} = \{-30, -32\}$ [dBm] (ramping-down), $a = 0.1$ [packets/slots], $p_\mathrm{a} = 0.6$, $\theta = -23$ [dBm].

unstable queue. Hence, considering the meta distribution is important to reveal information about the percentiles of stable and unstable nodes.

The results shown in Figs 2.9-2.12 are of primary importance to characterize the scalability-stability tradeoff in MWNs. In fact, the maximum spatial traffic density of nodes that can be accommodated subject to a γ-stability constraint is shown. For instance, Fig. 2.9 shows the (λ,a)-pairs that ALOHA with $p_\mathrm{a} = 0.3$ can accommodate while being subject to a given γ-stability constraint. The figure shows that accommodating more nodes may necessitate a lower traffic generation per-node to maintain the same γ fraction of stable nodes. The γ-stability of the network can also be controlled by enhancing the detection threshold of receivers as shown in Fig 2.10. The figure shows that, given a fixed a, to increase λ may require a lower threshold θ at the receivers in order to improve the success probabilities and cope with the increased spatial traffic density.

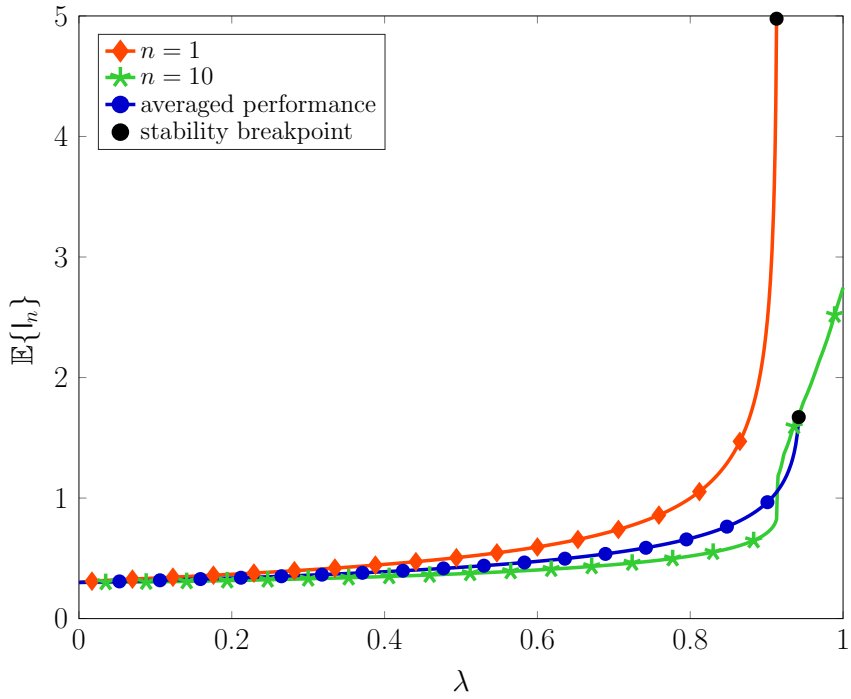

Figure 2.8: Average queuing length as a function of the node density for the low QoS-class (red diamonds), high QoS-class (green stars), and considering the spatial averages at the typical point (blue circles) for ALOHA with random channel selection with $N_c = 4$, $N = 10$, $a = 0.1$, $p_a = 0.4$, $\theta = -30$ [dB], $R = 10$ [m], $\eta = 2$, $\sigma^2 = -90$ [dBm], $\mathcal{P} = \{-30\}$ [dBm].

Fig 2.11 shows the importance of designing the ALOHA access through p_a to ensure a stable network operation by the regions on the (p_a,a)-plane where γ-stability holds for $\lambda = 0.1$ [node/m^2].

The figure shows that p_a must be greater than a to allow any fraction of the network to be stable, since a sufficiently persistent channel access is a necessary but not sufficient condition for stability. Note that for a given γ and increasing a, the minimum p_a ensuring γ-stability diverges increasingly from $p_a = a$. The Pareto frontier for region of the (p_a,λ)-pairs is shown in Fig 2.12. The figure shows that there is a given range of p_a that ensures stability for a given λ. This is because the tradeoff between conservative and aggressive channel access should be balanced to maintain stable queues. To employ a conservative access policy with low values of p_a misses many transmission opportunities, accumulates packets in buffers, and leads to instability. On the other hand, to employ an aggressive access policy with high values of

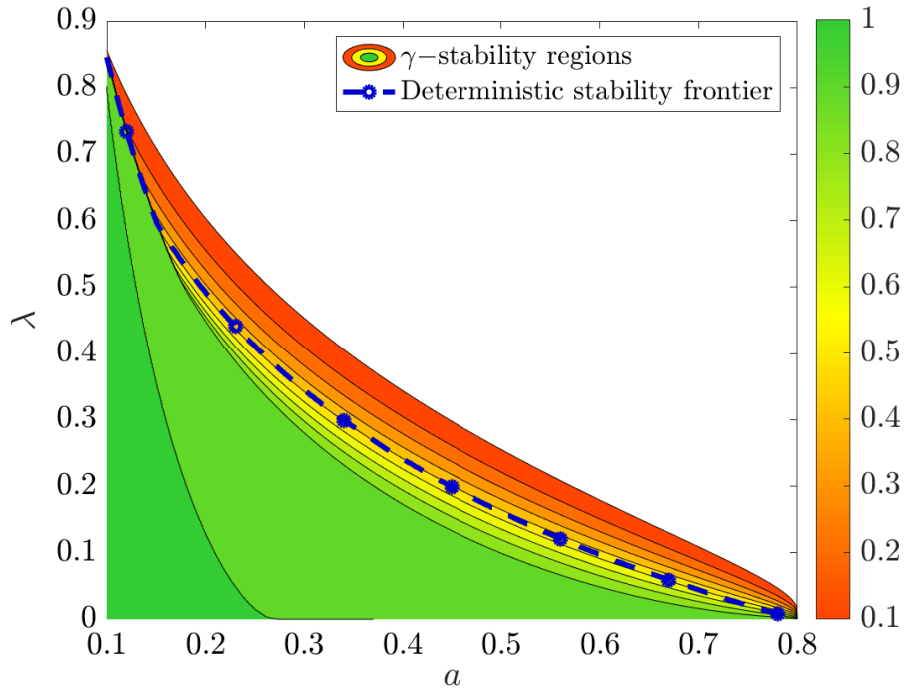

Figure 2.9: Stability regions of ALOHA with random channel selection over the (λ, a)-plane. We show the γ-stablity regions for $N = 10$ (colorplot) and the deterministic stability frontier for the average performance (marked dashed curve) for $N_{\mathrm{c}} = 4$, $\eta = 2$, $R = 10$ [m], $\theta = -30$ [dB], $\sigma^2 = -90$ [dBm], $\mathcal{P} = \{-30\}$ [dBm], and $p_{\mathrm{a}} = 0.8$ [attempts/slots].

p_{a} aggravates the interference, leads to excessive transmission failures due to low SINR, thus leading to instability.

Fig 2.13 shows the de facto Pareto frontiers, as well as the NC and SC frontiers, for different operational objectives of the considered uncoordinated MWN. Particularly, Fig 2.13 considers the uncoordinated MWN operation with (a) γ-stability for $\gamma = 0.99$ constraint, (b) γ-operativity for a delay $t^\star \leq 5$ [slots] and $\gamma = 0.5$, and (c) γ-operativity for a delay $t^\star \leq 3$ [slots] and $\gamma = 0.05$. The figure shows that the frontiers obtained by considering dominant systems, i.e., NC and SC conditions, do not provide tight upper and lower bounds, respectively, for the actual performance, which may either lead to a too conservative system operation with a lot of wasted resources or a too aggressive system with violated operational constraints. Particularly, operating with the SC constraints may lead to serving much lower intensity of nodes that the network can support. On the other hand, operating with

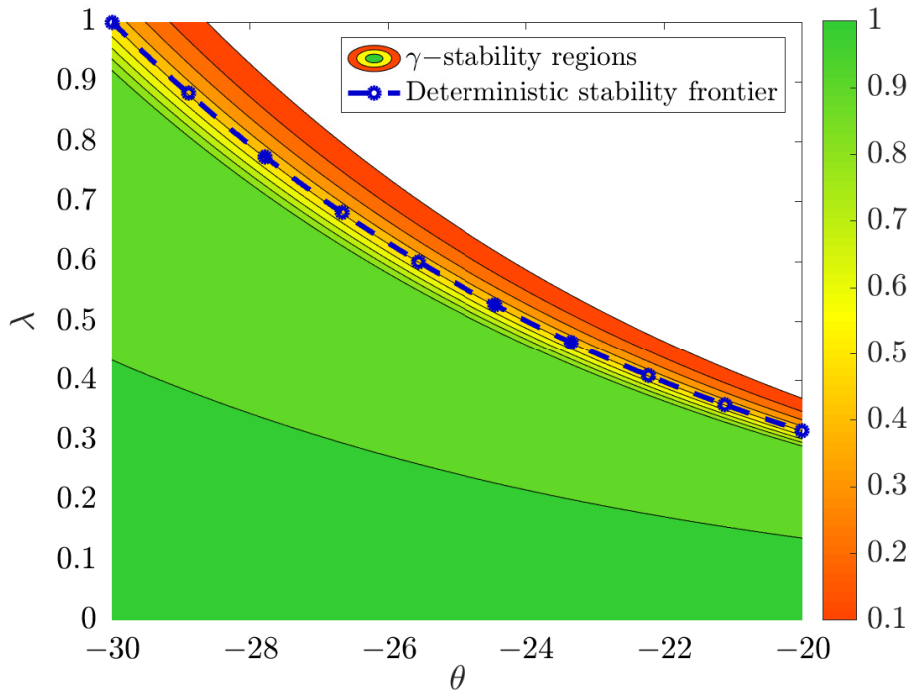

Figure 2.10: Stability regions of ALOHA with random channel selection over the (θ, λ)-plane. We show the γ-stablity regions for $N = 10$ (colorplot) and the deterministic stability frontier for the average performance (marked dashed curve) for $N_{\mathrm{c}} = 4$, $\eta = 2$, $R = 10$ [m], $\sigma^2 = -90$ [dBm], $\mathcal{P} = \{-30\}$ [dBm], $a = 0.1$ [packets/slots], and $p_{\mathrm{a}} = 0.3$.

the NC may result in serving a lot more nodes than the network should support but without any performance guarantee. Hence, Fig 2.13 manifests the importance of the developed spatiotemporal model to determine the network scalability under the required operational constraints.

To show the impact of the power-ramping strategy, we present a network design case study with $\lambda = 0.1$, $\theta = -23$ [dB], $\sigma^2 = -90$ [dBm], $a = 0.1$, $\eta = 2$, $R = 10$ [m] and $N = 10$. It is worth highlighting that the considered setting is according to LoRa dense ad-hoc scenario (10 nodes on a 10×10 [m^2] squared surface) for low-power consumption and short-range communications. Table 2.1 shows different design variations of ALOHA and the corresponding performance in terms of the fraction γ_{su} of stable nodes, the fraction γ_{to} of nodes with delay less than $t^\star$ time slots, and the fraction $\bar{w}_0$ of nodes with non-empty buffers. The results in the table emphasize that

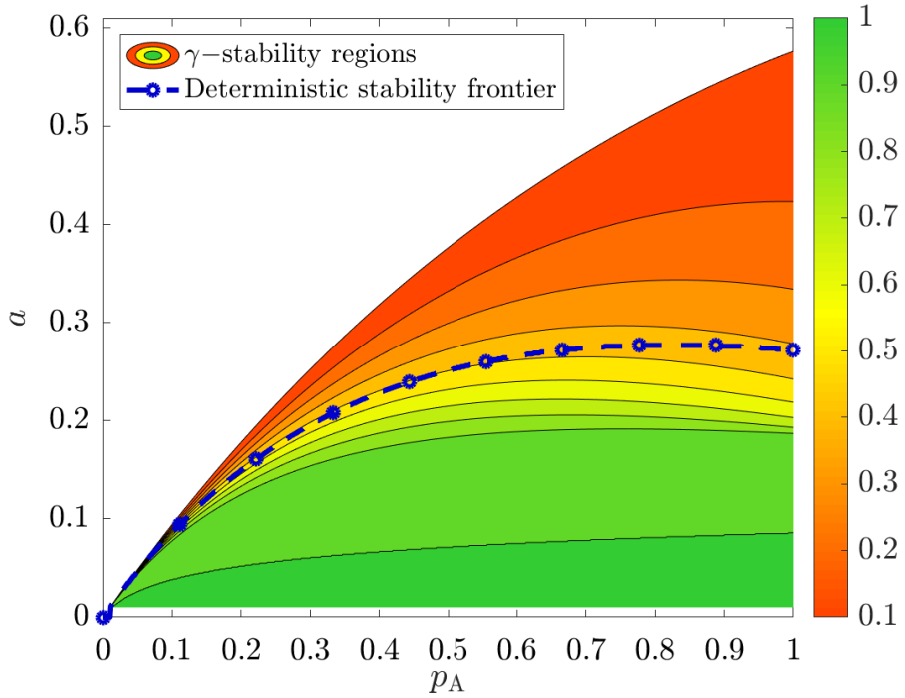

Figure 2.11: Stability regions of ALOHA with random channel selection over the (p_{a}, a)-plane. We show the γ-stablity regions for $N = 10$ (colorplot) and the deterministic stability frontier for the average performance (marked dashed curve) for $\lambda = 0.1$ [nodes/m^2], $N_{\mathrm{c}} = 4$, $\eta = 2$, $R = 10$ [m], $\theta = -30$ [dB], $\sigma^2 = -90$ [dBm], and $\mathcal{P} = \{-30\}$ [dBm].

ramping-down power control with some persistence on each power level outperforms all other schemes. This is because ramping-down the power reliefs the interference and the persistence on each power level ensures sacrificing the performance of nodes belonging to low QoS classes. Ramping-down without persistence may mistakenly degrade the performance of a node belonging to a high QoS class that experience instantaneously a severe fading. The table also manifests that ramping-up the power has the worst performance among all schemes, which is because ramping-up the power aggravates the interference without enhancing the performance of nodes at congested locations. The table also shows that the primitive single power ALOHA scheme outperforms the ramping-down scheme, which is not properly designed.

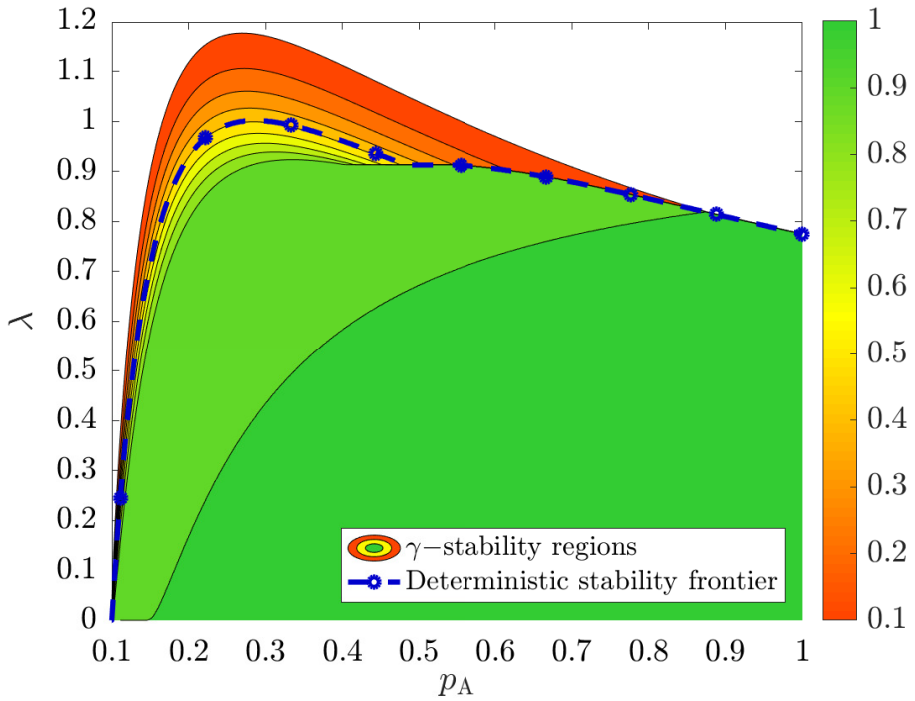

Figure 2.12: Stability regions of ALOHA with random channel selection over the (p_a, λ)-plane. We show the γ-stablity regions for $N = 10$ (colorplot) and the deterministic stability frontier for the average performance (marked dashed curve) for $N_c = 4$, $\eta = 2$, $R = 10$ [m], $\theta = -30$ [dB], $\sigma^2 = -90$ [dBm], $\mathcal{P} = \{-30\}$ [dBm], and $a = 0.1$ [packets/slots].

Table 2.1: Design of power ramping

	N_p	N_t	$\mathcal{P}$ [dBm]	γ_{su}	γ_{to} $t^\star = 5$	γ_{to} $t^\star = 10$	$w^{[0]}$
Single power	1	1	-30	0.4	0.1	0.4	0.15
Ramping-down 1	4	1	$-30, -32, -34, -40$	0.4	0	0.2	0.10
Ramping-down 2	4	10	$-30, -32, -34, -40$	0.6	0.2	0.5	0.25
Ramping-up 1	4	1	$-30, -28, -26, -22$	0.3	0	0.2	0.09
Ramping-up 2	4	10	$-30, -28, -26, -22$	0.2	0	0.2	0.06

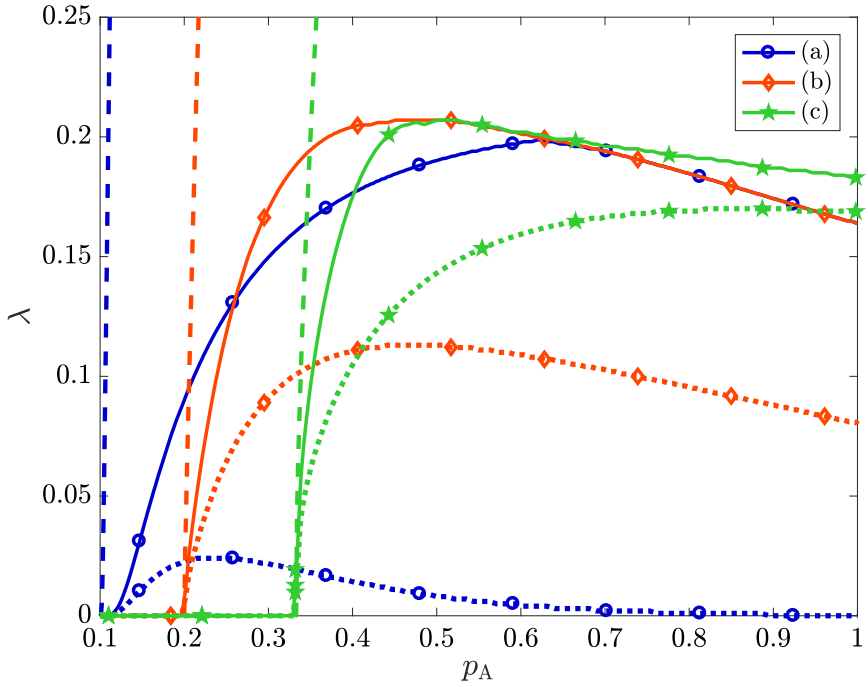

Figure 2.13: Pareto frontiers for the necessary (dashed), sufficient (dotted), and actual (solid) conditions for simple ALOHA for (a): γ-stability, with $a = 0.1$ and $\gamma = 0.999$; (b): γ-operativity, with $t^\star = 5$ [slots] and $\gamma = 0.5$; and (c): γ-operativity, with $t^\star = 3$ [slots] and $\gamma = 0.05$. We considered $\eta = 2$, $R = 10$ [m], $\theta = -30$ [dB], $\sigma^2 = -90$ [dBm], $\mathcal{P} = \{-30\}$ [dBm], and $a = 0.1$ [packets/slots].

2.7 Final Remarks

The analysis of this chapter combines stochastic geometry and queuing theory to develop a novel holistic spatiotemporal modeling for uncoordinated MWNs. We carry out both the macroscopic- and microscopic-scale analysis through a converging iterative proceidure that keeps track of the number of packets in the transmitter buffers, channel access, transmission power, and the retransmission phase. We neglect the simplistic assumption of high mobility, and consider fixed node locations for the analysis, thus accounting for interference temporal correlation. Our framework goes beyond the analysis through spatial averages at the typical point of the network and accounts for the metadistribution of the SINR, which enables the characterization of the location-dependent performance by the partitioning of the networkinto

N QoS-classes. By such a partitioning we compute the percentile of stable nodes and the percentile of nodes achieving a target operation in terms of delay or queuing length, thus introducing the concepts of γ-stability and γ-operativity. The stability-scalability and operativity-scalability tradeoffs are shown via the Pareto frontiers of the γ-stability and γ-operativity regions, respectively, by accounting for the per-node traffic intensity, node density, target transmission rate, and uncoordinated access persistence. Our results also show that the Pareto frontier retrieved from the spatial averaging at the typical point, corresponds to a total uncertainty on the actual fraction of network holding stability (or target operation), thus proving the superiority of our analysis. Further, for both stability and operativity, we show that the Pareto frontiers obtained for the necessary and sufficient conditions corresponding to two dominant systems are not tight bounds of the actual frontier obtained through our framework, thus highlighting that, towards accounting for spatiotemporal interactions among queues, it is mandatory to consider the location-dependent performance of each queue, while it is inaccurate to account for dominant systems. Further, variations of the F-ALOHA protocol with different power-ramping schemes are presented to improve the γ-stability and γ-operativity. The importance of power-ramping design is manifested through a case study that shows that ramping-down the power after a properly designed number of retrials can improve the network percentile performance.

Chapter 3

Intrinsic Secrecy in Inhomogeneous Stochastic Networks

3.1 Preliminaries

Network intrinsic secrecy is the capacity of a network to hide a portion of the transmitted information from unwanted listeners by solely relying on the physical properties of the wireless channel. Its exploitation is a key enabler for several emerging wireless applications including operation and control of cyber-physical systems [151–153], IoT [30, 154, 155], and vehicular networks [156–158].

3.1.1 Big Picture

The need for communication confidentiality has existed since antiquity. A simple and famous example is the Caesar cipher, used by Julius Caesar according to Suetonius for protecting missives of military significance [159]. Nowadays the confidentiality of wireless communications has become crucial due to the advent of pervasive wireless networks and the development of secrecy-sensible applications. In fact, the broadcast nature of the wireless channel facilitates the information eavesdropping; on the other hand, it offers the possibility to exploit network interference to enhance the secrecy level.

Information-theoretic secrecy has emerged in the broader area of physical layer security [72] as a possible solution to complement the traditional cryptographic techniques [160–163]. In recent studies based on the seminal work of Shannon [70] and Wyner [164], it is highlighted how network intrinsic features such as wireless propagation medium, node locations, and aggregate interference impact network secrecy [74]. Such an analysis high-

Figure 3.1: Voltone del Podestà in Piazza Maggiore, Bologna, Italy.

lights the usability of network interference to obtain secrecy enhancement. Interference engineering strategies (IESs) can be devised to imbalance the quality of the legitimate and eavesdropping links and, thus, to obtain confidential communications at a non-zero rate. In particular, the node spatial distribution is crucial for the level of confidentiality in the network. Fig. 3.1 shows the Voltone del Podestà in Bologna, which is an example of intrinsic confidentiality of the communication. In particular, only persons at two opposite columns can hear each others speech due to the peculiar shape of the structure.

3.1.2 Related Works and Motivation

The seminal work of Wyner introduces the secrecy capacity of a wire-tap channel [164]. After the characterization of the discrete memoryless channel, secrecy capacity is studied in Gaussian wire-tap channels [165], in fading channels [166], in the presence of interference [167], with multi-antenna links [168], for multilevel networks [111], and with eavesdropper collusion [112].

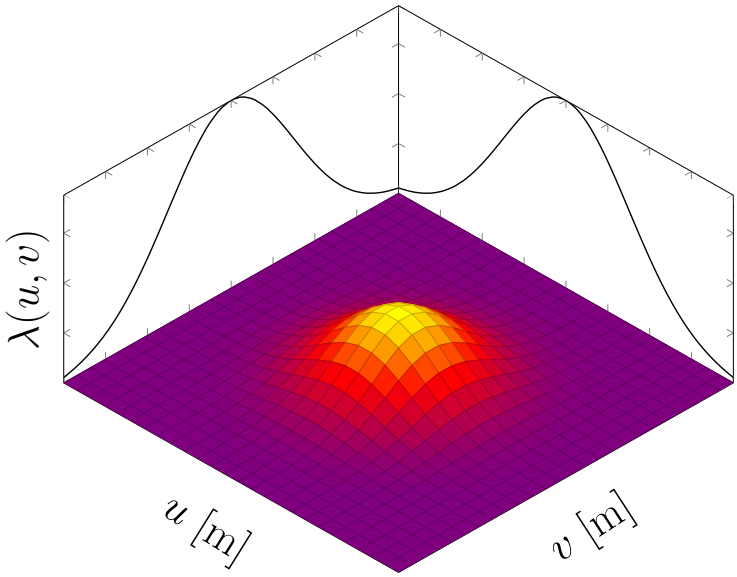

Figure 3.2: Intensity function.

Recently, IESs have been proposed to enhance the secrecy of small networks consisting of source, destination, helping nodes and eavesdroppers. Techniques like artificial noise [73, 169], artificial noise alignment [170, 171], friendly jamming [172,173], and cooperative jamming [75,174,175] have been developed to impair the eavesdropping channel and, hence, achieve a non-zero secrecy rate at the legitimate receiver. Generalized interference alignment techniques that maximize network secrecy for large-scale stochastic networks have been proposed in [109, 110].

Other recent works explore information-theoretic secrecy in generic [76–78], cellular [79–82], D2D enabled [83,84], full-duplex enabled [85], and multi-tier [86] large-scale networks with stochastic topology. Such papers consider the homogeneous Poisson point process (HPPP) for modeling node spatial distributions, which has been extensively adopted to study the role of aggregate interference in wireless networks [93, 129, 176, 177] because of its tractability. However, the HPPP cannot capture practical scenarios that may involve spatial clustering, space dependent access control, and non-uniform mobility.

Several types of stationary point processes have been introduced to study wireless networks with spatial correlation, e.g., Cox, cluster, hardcore, Gibbs, and determinantal point processes [143, 178, 179]. Such point processes account for properties like attraction, repulsion, and regularity in node patterns

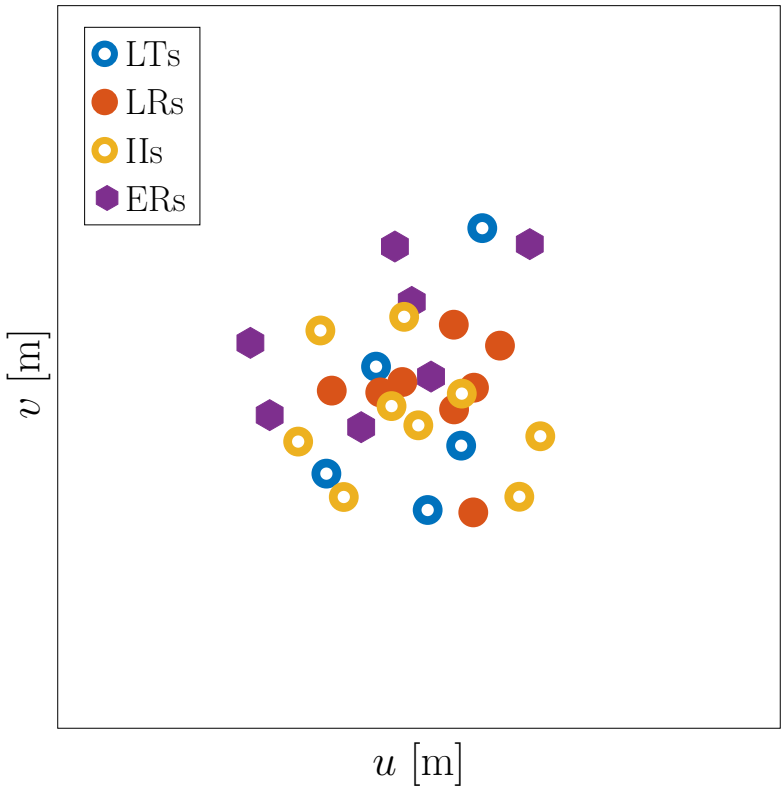

Figure 3.3: Realization.

and are particularly useful to study the spatial distribution both of clustered and cellular networks [180, 181]. Such stationary models have the advantage of being able to describe the average performance of the network in a tractable way. Nevertheless, such translation invariant models have the main limitation of not being capable of describing the location-dependent performance within a network. For this reason we consider inhomogeneous point processes to tackle the spatial variability of the network performance when a spatial model of node density is available. This has found application in different scenarios such as mobile, vehicular, and sensor networks [182–186]

Consider a clustered network, when classical homogeneous Poisson cluster model is used it is only possible to determine the average performance at the typical point of the clustered network. In particular, a receiver can be considered at any point in any cluster, and the statistics evaluated at that point represent the average statistic over all point configurations [113]. The analysis developed in this chapter considers inhomogeneous Poisson cluster and enables to determine the performance variations while moving within a clus-

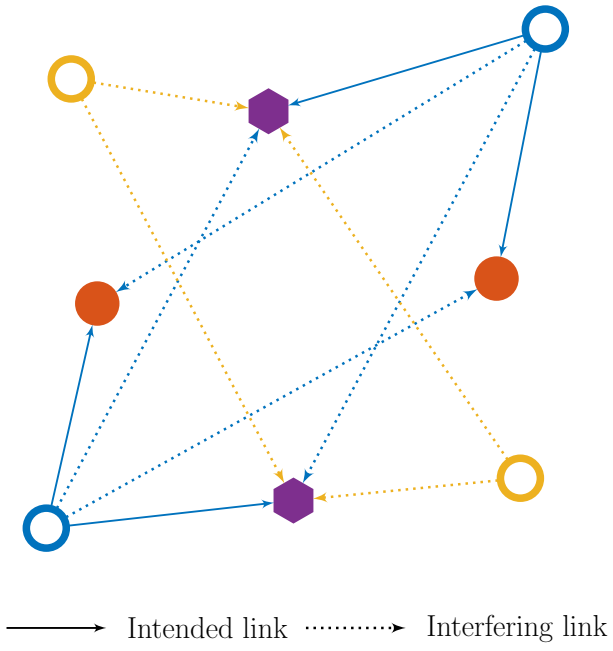

Figure 3.4: System model.

ter and from cluster to cluster. Thus, we aim to provide a spatial description of secrecy metrics, to consider the inhomogeneous distribution of the nodes. Furthermore, secrecy needs to be guaranteed over the whole network, and the analysis at a typical point is inadequate. Therefore, it is important to study the *inhomogeneous network* where nodes are spatially distributed according to an inhomogeneous Poisson point process (IPPP) (see Fig. 3.2-3.3). The considered setting represents a challenging generalization with respect to (w.r.t.) the homogeneous one, especially for what concerns the characterizations of the interference and SINR when a destination selection policy is employed.

3.1.3 Contribution

This chapter, which is in part presented in [2,5], provides foundations for the analysis of intrinsic secrecy in inhomogeneous wireless networks. We propose a framework based on the characterization of the signal-to-interference ratio (SIR) which accounts for 1) the spatial distributions of LTs, legitimate receivers (LRs), eavesdropping receivers (ERs), and intentional interferers (IIs); 2) the wireless propagation medium; and 3) the aggregate interference at each receiver. We consider three scenarios: the full inhomogeneous

Table 3.1: Notation used throughout the chapter.

Symbol	Usage
$\mathcal{A} \subseteq \mathbb{R}^d$	Bounded Borel set in $\mathbb{R}^d$
$\mathsf{i},\ i$	Random variable and its realization
$\mathsf{x},\ \boldsymbol{x}$	Random vector and its realization
$\Pi,\ \mathit{\Pi}$	Point process and its realization
$\mathbb{1}_Y(\cdot)$	Indicator function for the property Y
$\Pi(\mathcal{A}) = \mathsf{n}_{\mathcal{A}}$	Number of points in $\mathcal{A}$
$\lambda(\cdot)$	Intensity function [nodes/m^d]
$\Lambda(\cdot)$	Intensity measure over $\mathcal{A}$ [nodes]
$\mathbb{S}\{\cdot\}$	Destination selection operator
$\mathbb{E}\{\cdot\}$	Expectation operator
$\mathbb{P}\{\cdot\}$	Probability operator
$\mathbb{E}^{!j}\{\cdot\}$	Reduced Palm expectation given $\boldsymbol{x}_j$
$\mathcal{T},\ \mathcal{J}$	Index sets of LTs and IIs
$\mathcal{R}_j$	Index set of receivers of $\boldsymbol{x}_j$
$\mathcal{E}_j$	Index set of eavesdroppers of $\boldsymbol{x}_j$
$k \in \mathcal{R}_j$	index of the generic receiver of $\boldsymbol{x}_j$
$\bar{k} = \mathbb{S}\{\mathcal{R}_j\}$	Index of the receiver selected by $\boldsymbol{x}_j$
(k)	Index of the k^{th} closest LR to $\boldsymbol{x}_j$
$\breve{k}$	Index of the maximum SIR LR of $\boldsymbol{x}_j$
$\mathsf{i}_{j,k}$	Interference at x_k given $\boldsymbol{x}_j$
$\mathsf{i}_{j,k}\vert\mathsf{x}_k$	Interference at $\boldsymbol{x}_k$ given $\mathsf{x}_j = \boldsymbol{x}_j$
$f_{\mathsf{z}}(\cdot)$	PDF of the RV z
$F_{\mathsf{z}}(\cdot)$	CDF of the RV z
$\psi_{\mathsf{i}}(\cdot)$	CF of the RV i
$\mathcal{L}_{\mathsf{i}}(\cdot)$	Laplace transform of the RV i
$\mathsf{r}_{j,(k)}$	Distance between $\boldsymbol{x}_j$ and its k^{th} closest LR
$\varphi_{j,\bar{k},\breve{l}}$	MSR of at the selected LR of $\boldsymbol{x}_j$
$\mathcal{U}(a,b]$	Uniform distribution on the interval $(a,b]$
$\mathcal{P}(a)$	Poisson' distribution with parameter a
$\Vert\cdot\Vert,\ \vert\cdot\vert$	Euclidean norm, Lebesgue measure
$\Re\{c\}$	Real part of $c \in \mathbb{C}$

network (FIN), full homogeneous networ (FHN), and partial inhomogeneous

network (PIN). The key contributions of the work can be summarized in the following actions:

- develop a framework for the design and analysis of inhomogeneous wireless networks with intrinsic secrecy composed of legitimate nodes, intentional interferers, and eavesdroppers with inhomogeneous distributions;
- characterize the statistic of the received SIR in legitimate and eavesdropping networks for different receiver selection strategies in the FIN, FHN, and PIN scenarios;
- define local and global secrecy metrics for inhomogeneous networks;
- quantify the secrecy performance in different scenarios with physical interpretations of different inhomogeneities.

Our approach combines information theory, communication theory, probability theory, and stochastic geometry to develop a theoretical analysis corroborated by simulations in different network settings. The novelty of the work is in the analysis of the location-dependent performance of the network, which allows to characterize accurately the different local secrecy levels arising from the diverse local node densities. We then show how the availability of an inhomogeneous model that reflects the spatial characteristics of a network allows to accurately unveil the local performance. The main difficulty is to hold tractability while considering the intricate relations between the distributions of LTs, LRs, ERs, and IIs. This makes difficult to characterize the aggregate interference and the SINR. Nevertheless, we devise a systematic procedure to characterize and compute key performance indicators for any destination selection policy by means of numerical integrations.

3.1.4 Notation and Organization

Notation

The notations used in this chapter is summarized in Table 3.1.

Organization

The rest of the chapter is organized as in the following: Section 3.2 presents the network model. Section 3.3 analyzes the aggregate interference distribution in inhomogeneous networks. Section 3.4 develops the statistical characterization of the received SIR in generic and Nakagami-m fading channels for different destination selection strategies. Section 3.5 defines local and global

secrecy metrics for inhomogeneous networks. Section 3.6 proposes competitive strategies based on node inhomogeneous stochastic deployment as case studies. Section 3.7 provides numerical results and section 3.8 gives our final remarks.

3.2 Network Model

Consider four overlaid networks as in Fig. 3.4: the legitimate transmitter network (LTN); legitimate receiver network (LRN); eavesdropping receiver network (ERN); and intentional interferer network (IIN). These networks are modeled via independent IPPPs defined over an d-dimensional Euclidean space. Recall that a point process Π is defined over a bounded Borel set[1] $\mathcal{A} \subseteq \mathbb{R}^d$ and has the twofold nature of being a random measure, i.e., the number of points in $\mathcal{A}$, $\Pi(\mathcal{A}) = \mathsf{n}_{\mathcal{A}}$, and a random sequence of points, i.e., $\Pi = \{\mathbf{x}_1, \mathbf{x}_2, \dots\} = \{\mathbf{x}_{\mathsf{n}_{\mathcal{A}}}\}$. Further, Π is characterized by the intensity function $\lambda(\boldsymbol{x})$ for all $\boldsymbol{x} \in \mathcal{A}$ or, equivalently, by the intensity measure $\Lambda(\mathcal{A})$, where[2]

$$\Lambda(\mathcal{A}) = \int_{\mathcal{A}} \lambda(\boldsymbol{x}) d\boldsymbol{x} \,.$$

The considered networks are described in the following points.

- The LTN and the LRN form the legitimate network, which consist of nodes exchanging confidential information. The LTN and the LRN are denoted by the point processes Π_{tx} and Π_{rx} with intensity functions $\lambda_{\text{tx}}(\boldsymbol{x})$ and $\lambda_{\text{rx}}(\boldsymbol{x})$, respectively.

- The ERN is composed of malicious nodes trying to intercept the confidential information exchanged through the legitimate network. It is described by the point process Π_{ex} with intensity function $\lambda_{\text{ex}}(\boldsymbol{x})$.

- The IIN is made up of nodes that introduce jamming messages in the radio channel to impair the ERs' channels. The IIN is described by the point process Π_{jx} with intensity function $\lambda_{\text{jx}}(\boldsymbol{x})$.

[1] A Borel set is the smallest σ-algebra on $\mathbb{R}^d$ that contains all the open subsets of $\mathbb{R}^d$ [189].

[2] The intensity function of point processes represents the density of nodes per unit area and is measured in [nodes/m^d]. The intensity measure is the mean number of points of Π on $\mathcal{A}$.

We model the point processes of interferers affecting the LRs and ERs as IPPPs with intesity functions given, respectively, by

$$\lambda_{\mathrm{ir}}(\boldsymbol{x}) = \beta_{\mathrm{tr}}\lambda_{\mathrm{tx}}(\boldsymbol{x}) + \beta_{\mathrm{jr}}\lambda_{\mathrm{jx}}(\boldsymbol{x}) \tag{3.1a}$$

$$\lambda_{\mathrm{ie}}(\boldsymbol{x}) = \beta_{\mathrm{te}}\lambda_{\mathrm{tx}}(\boldsymbol{x}) + \beta_{\mathrm{je}}\lambda_{\mathrm{jx}}(\boldsymbol{x}) \tag{3.1b}$$

where the parameters $\beta_{\mathrm{tr}}, \beta_{\mathrm{te}}, \beta_{\mathrm{jr}}, \beta_{\mathrm{re}} \in [0, 1]$ model the capability of the subnetworks to control the interference. Specifically, at the receivers' side interference cancellation can be employed if the sequence of transmitted symbols is known, while at the transmitters' side interference alignment can be exploited to null the interference at some specific locations via multiple antennas [**?**]. For the sake of simple presentation, in the rest of the paper we consider no interference cancellation nor interference alignment for the LTs' interference (i.e., $\beta_{\mathrm{tr}} = \beta_{\mathrm{te}} = 1$), no interference cancellation nor alignment for the IIs' interference at the ERs (i.e., $\beta_{\mathrm{je}} = 1$), and perfect cancellation or alignment for the IIs' interference at the LRs (i.e., $\beta_{\mathrm{jr}} = 0$). In such a scenario, the LRs know the sequence of symbols transmitted by the IIs or IIs use multiple antennas to align the interference at ERs locations. Therefore, the interferers affecting the LRN and the ERN are described by the point processes Π_{ir} and Π_{ie} with intensity functions $\lambda_{\mathrm{ir}}(\boldsymbol{x}) = \lambda_{\mathrm{tx}}(\boldsymbol{x})$ and $\lambda_{\mathrm{ie}}(\boldsymbol{x}) = \lambda_{\mathrm{tx}}(\boldsymbol{x}) + \lambda_{\mathrm{jx}}(\boldsymbol{x})$, respectively. Section 2.6 considers the case wherein the ERs knows the sequence of symbols of the IIs and perform interference cancellation (i.e., $\lambda_{\mathrm{ie}}(\boldsymbol{x}) = \lambda_{\mathrm{tx}}(\boldsymbol{x})$).

Let $\mathcal{T}$ and $\mathcal{J}$ denote the index sets of LTs and IIs, respectively. For the j^{th} LT in $\mathcal{T}$, $\mathcal{R}_j$ denotes the index set of potential LRs and $\mathcal{E}_j$ the index set of ERs. For a specific legitimate link, $k \in \mathcal{R}_j$ is the receiver index. Similarly, for an eavesdropping link, $i \in \mathcal{E}_j$ is the ER index.

3.3 Interference Panorama in Inhomogeneous Wireless Networks

In wireless networks, noise and interference are important for determining the performance of communications. In interference-limited systems the additive noise is considered negligible w.r.t. the aggregate interference. Therefore, we neglect the effect of the noise and assume an interference-limited regime.

It is well known that the interference distribution at a given point of a network can be described by the characteristic function or equivalently by the Laplace transform [189]. When the network is modeled as an HPPP, the interference distribution is the same at each location [93]; otherwise, the analysis presents remarkable difficulties.

$$\psi_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(\jmath\omega) = \exp\Bigg\{ - \int_{\mathcal{A}} \Big(1 - \psi_{\mathsf{h}}\Big(\jmath\omega\big((u-u_j-r_{j,k}\cos\theta_{j,k})^2 + (v-v_j-r_{j,k}\sin\theta_{j,k})^2\big)^{-b}\Big)\Big)\lambda_{\mathrm{tx}}(u,v)dudv\Bigg\} \tag{3.9}$$

We introduce a random link composed of a transmitter $\boldsymbol{x}_j$ and a receiver $\mathsf{x}_k \in \Pi_{\mathrm{rx}}$ in $\mathcal{A} \subseteq \mathbb{R}^d$.[3] The signal power received by x_k is

$$\mathsf{p}_{j,k} = p_{\mathrm{T}}|\mathsf{s}_j|^2 \frac{\mathsf{h}_{j,k}}{\mathsf{r}_{j,k}^{2b}} \tag{3.2}$$

where p_{T} is the transmitted power, $|\mathsf{s}_j|^2$ is the power of the complex transmitted symbol, b is the amplitude path-loss exponent, $\mathsf{h}_{j,k} \in \mathbb{C}$ is the quasi-static channel power gain and $\mathsf{r}_{j,k} = \|\boldsymbol{x}_j - \mathsf{x}_k\|$ is the Euclidean distance between the locations $\boldsymbol{x}_j$ and x_k. The aggregate interference power level at x_k is expressed by

$$\mathsf{i}_{j,k} = \sum_{\mathsf{x}_q \in \Pi_{\mathrm{ir}}} p_{\mathrm{T}}|\mathsf{s}_q|^2 \frac{\mathsf{h}_{q,k}}{\mathsf{r}_{q,k}^{2b}}\,. \tag{3.3}$$

In the following we consider $p_{\mathrm{T}} = 1$, $|\mathsf{s}|^2 = 1$, and i.i.d. channel power gains.[4] Further, $\mathsf{i}_{j,k}$ is a RV taking different values for each realization of point processes and channels. The conditional characteristic function of the interference at a given location can be expressed by means of the probability generating functional (PGFL) of the PPP [189] as

$$\psi_{\mathsf{i}_{j,k}|\mathsf{x}_k}(\jmath\omega) = \exp\left\{ - \int_{\mathcal{A}} \left(1 - \psi_{\mathsf{h}}\left(\frac{\jmath\omega}{\|\boldsymbol{x} - \boldsymbol{x}_k\|^{2b}}\right)\right)\lambda_{\mathrm{ir}}(\boldsymbol{x})d\boldsymbol{x}\right\} \tag{3.4}$$

where $\jmath$ is the imaginary unit.
It is worth noting a particular feature of the inhomogeneous network: the statistical distribution of the aggregate interference is different in each possible realization of the random location x_k of the receiver. This is because

[3]The notation $\mathsf{x}_k \in \Pi_{\mathrm{tx}}$ indicates that the random points x_k belongs to a random sequence Π_{tx}, exploiting the nature of Π_{tx} of being a random sequence of points in $\mathcal{A} \subseteq \mathbb{R}^d$.

[4]Consider that every LT and IIs transmit symbols s_j and s_q, respectively, with symbol $|\mathsf{s}_j|^2 = |\mathsf{s}_q|^2 = |\mathsf{s}|^2 = 1$ for all $j \in \mathcal{T}$ and $q \in \mathcal{J}$. For all pairs of locations $\boldsymbol{x}_j, \boldsymbol{x}_k \in \mathcal{A}$, the same square channel gain distribution is assumed, i.e., $\psi_{\mathsf{h}_{j,k}}(\cdot) = \psi_{\mathsf{h}}(\cdot)$, in terms of characteristic functions.

from each location $\boldsymbol{x}_k$ we see a different *panorama of interferers*, which is the distribution of the interferers seen from x_k.

We now introduce the unconditional characteristic function of the interference, which is useful when an SIR analysis is carried out considering a destination selection strategy, as will be shown in Section 3.4. The unconditional characteristic function is obtained by marginalizing $\psi_{\mathsf{i}_{j,k}|\mathsf{x}_k}(\jmath\omega)$ over the spatial PDF $f^{\mathrm{rx}}_{\mathsf{x}_k}(\boldsymbol{x})$ of the receiver's location x_k as

$$\psi_{\mathsf{i}_{j,k}}(\jmath\omega) = \mathbb{E}_{\mathsf{x}_k}\{\psi_{\mathsf{i}_{j,k}|\mathsf{x}_k}(\jmath\omega)\} \tag{3.5}$$

where

$$f^{\mathrm{rx}}_{\mathsf{x}_k}(\boldsymbol{x}) = \frac{\lambda_{\mathrm{rx}}(\boldsymbol{x})}{\Lambda_{\mathrm{rx}}(\mathcal{A})} \tag{3.6}$$

for all $\boldsymbol{x} \in \mathcal{A}$. For a receiver selected randomly, according to the spatial distribution in (3.6), $\psi_{\mathsf{i}_{j,k}}(\jmath\omega)$ is independent from $\boldsymbol{x}_j$, i.e., $\psi_{\mathsf{i}_{j,k}}(\jmath\omega) = \psi_{\mathsf{i}}(\jmath\omega)$.

To consider other receiver selection strategies than the random one, it is convenient to express the marginalization and the spatial distribution of (3.5) and (3.6) w.r.t. the polar coordinates of $\boldsymbol{x}_k$. For networks in $\mathcal{A} \subseteq \mathbb{R}^2$, the position $\boldsymbol{x}_k$ can be conveniently expressed by means of its polar coordinates w.r.t. the position $\boldsymbol{x}_j$, i.e.,

$$\boldsymbol{x}_k = \begin{bmatrix} u_k \\ v_k \end{bmatrix} = \begin{bmatrix} u_j + r_{j,k}\cos\theta_{j,k} \\ v_j + r_{j,k}\sin\theta_{j,k} \end{bmatrix} . \tag{3.7}$$

Then (3.5) takes the form of

$$\psi_{\mathsf{i}_{j,k}}(\jmath\omega) = \mathbb{E}_{\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}\{\psi_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(\jmath\omega)\} \tag{3.8}$$

where $\psi_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(\jmath\omega)$ is defined in (3.9) and the expectation is performed w.r.t. the joint PDF of $\mathsf{r}_{j,k}$ and $\boldsymbol{\theta}_{j,k}$, i.e., $f_{\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(r_{j,k},\theta_{j,k})$. As will be shown in the following section, this model simplifies the statistical analysis of the received SIR for the considered receiver selection strategies.

Recall that if the interferers are uniformly distributed over $\mathcal{A} = \mathbb{R}^2$, the distribution of the aggregate interference does not depend on the location where it is evaluated [93], i.e.,

$$\psi_{\mathsf{i}_{j,k}|\mathsf{x}_k}(\jmath\omega) = \psi_{\mathsf{i}_{j,k}}(\jmath\omega) \tag{3.10a}$$

$$= \exp\left(-\lambda_{\mathrm{ir}}\gamma|\omega|^{\frac{1}{b}}\left[1 + \frac{\jmath\omega}{|\jmath\omega|}\tan\left(\frac{\pi}{2b}\right)\right]\right) \tag{3.10b}$$

for all $\boldsymbol{x}_k \in \mathcal{A}$. Then, $\mathsf{i}_{j,k}$ belongs to the class of *skewed stable* RVs

$$\mathsf{i}_{j,k} \sim \mathcal{S}\left(\frac{1}{b}, 1, \lambda_{\mathrm{ir}}\gamma\right) \tag{3.11}$$

where

$$\gamma = \pi B_{\frac{1}{b}}^{-1} \mathbb{E}\left\{ \mathsf{h}^{\frac{1}{b}} \right\} \tag{3.12}$$

$$B_a = \begin{cases} \frac{1-a}{\Gamma(2-a)\cos\left(\frac{\pi a}{2}\right)} & \text{for } a \neq 1 \\ \frac{2}{\pi} & \text{for } a = 1 \end{cases} \tag{3.13}$$

and where $\Gamma(\cdot)$ is the Gamma function.

3.4 Statistical Characterization of SIR

In interference-limited systems, the additive noise is considered as negligible w.r.t. the aggregate interference level. For this reason we analyze performance by means of the SIR

$$\mathsf{z}_{j,k} \triangleq \frac{\mathsf{h}_{j,k}}{\mathsf{r}_{j,k}^{2b} \mathsf{i}_{j,k}}. \tag{3.14}$$

Different destination selection strategies are taken into account for characterizing the SIR of a legitimate link. In particular, the confidential information can be sent to: 1) a randomly selected receiver, 2) the receiver with maximum SIR, or 3) the k^{th} closest receiver. Regarding the eavesdropping link, we consider only the ER with maximum instantaneous SIR, i.e., the most dangerous and limiting for secrecy performance.

3.4.1 SIR in the Legitimate Network

For a transmitter located in $\boldsymbol{x}_j$, we characterize the SIR received by the LR at $\mathbf{x}_{\bar{k}}$ with index $\bar{k} = \mathbb{S}\{\mathcal{R}_j\}$, i.e., which is selected within $\mathcal{R}_j$ using the selection strategy $\mathbb{S}\{\cdot\}$. Note that this characterization is local and is conditioned on the transmitter location. The analysis generalizes the results of [76] to inhomogeneous wireless networks. In particular, we extend in Lemmas 1 and 2 results obtained in Sections IV and V of [76], respectively.

Randomly Selected Receiver

Hereafter we provide two lemmas to characterize the distribution of the SIR given a random selection policy.

Lemma 1 (*Random link SIR distribution in fading channels*) *Let* $\mathbf{x}_k \in \Pi_{\text{rx}}$ *be the location of the receiver randomly selected by the transmitter in* $\boldsymbol{x}_j$

$$\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\boldsymbol{\theta}_{j,k}}(s\,m\,r_{j,k}^{2b}z) = \exp\left\{-\int_{\mathcal{A}}\left(1-\left(\frac{\left((u-u_j-r_{j,k}\cos\theta_{j,k})^2+(v-v_j-r_{j,k}\sin\theta_{j,k})^2\right)^b}{\overline{\Omega}\,s\,{r_{j,k}}^{2b}z+\left((u-u_j-r_{j,k}\cos\theta_{j,k})^2+(v-v_j-r_{j,k}\sin\theta_{j,k})^2\right)^b}\right)^m\right)\frac{\Lambda_{\mathrm{tx}}(\mathcal{A})}{2\pi\sigma^2}e^{-\frac{u^2+v^2}{2\sigma^2}}dudv\right\} \tag{3.22}$$

---

according to the spatial PDF described in (3.6). The CDF of the SIR $\mathsf{z}_{j,k}$ *is given by*

$$F_{\mathsf{z}_{j,k}}(z) = \frac{1}{2}+\frac{1}{\pi}\int_0^\infty \Re\Big\{\frac{\psi_{\mathsf{g}_{j,k}}(\jmath\omega)}{\jmath\omega}\Big\}d\omega \tag{3.14a}$$

$$\psi_{\mathsf{g}_{j,k}}(\jmath\omega) = \psi_{\mathsf{h}_{j,k}}(\jmath\omega)\mathbb{E}_{\mathbf{x}_k}\left\{\psi_{\mathsf{i}_{j,k}|\mathbf{x}_k}\left(-\jmath\omega\mathsf{r}_{j,k}^{2b}z\right)\right\} \tag{3.14b}$$

where $\mathsf{g}_{j,k} \triangleq \mathsf{h}_{j,k} - z\mathsf{r}_{j,k}^{2b}\mathsf{i}_{j,k}$ *and* $\psi_{\mathsf{i}_{j,k}|\mathbf{x}_k}(\cdot)$ *is given by (3.4).*

Proof 3 *The proof follows directly from the Gil-Pelaez inversion theorem [190]; then, exploiting the independence between the useful channel gain and the interference. The steps of the proof are similar to those in Sections IV-A1, IV-A2, and Appendix B of [76], except for the generalization*

$$\mathbb{E}_{\mathsf{r}_{j,k}}\left\{\psi_{\mathsf{i}_{j,k}}\left(-\jmath\omega\mathsf{r}_{j,k}^{2b}z\right)\right\} \quad = \quad \mathbb{E}_{\mathbf{x}_k}\left\{\psi_{\mathsf{i}_{j,k}|\mathbf{x}_k}\left(-\jmath\omega\|\boldsymbol{x}_j-\boldsymbol{x}_k\|^{2b}z\right)\right\}. \tag{3.15}$$

□

Lemma 2 (*Generic link SIR distribution in Nakagami-m fading channels*) *For the scenario of Lemma 1 with Nakagami-m fading channels, the CDF of* $\mathsf{z}_{j,k}$ *is given by*

$$F_{\mathsf{z}_{j,k}}(z) \quad = \quad 1 \; - \; \sum_{i=0}^{m-1}\frac{(-1)^i}{i!}\left[\frac{d^{(i)}}{ds^i}\mathbb{E}_{\mathbf{x}_k}\left\{\mathcal{L}_{\mathsf{i}_{j,k}|\mathbf{x}_k}\left(s\,m\,r_{j,k}^{2b}z\right)\right\}\right]_{s=1} \tag{3.16}$$

where $s\in\mathbb{C}$*, and* $\mathcal{L}_{\mathsf{i}_{j,k}|\mathbf{x}_k}(\cdot)$ *is the conditional Laplace transform of the interference obtained by plugging into (3.4)*[5]

$$\mathcal{L}_{\mathsf{i}}(s) = \psi_{\mathsf{i}}(\jmath\omega)\big|_{\jmath\omega=-s}. \tag{3.17}$$

[5]Note that the Laplace transform and the characteristic function of the aggregate interference are both deducted by the probability generating functional [189].

Proof 4 *The proof follows directly by considering the exponential distribution of the useful channel gain, which allows to use the Laplace transform of the interference. The steps of the proof are similar to those in Section V-A and Appendix D of [76].* □

Note that (3.14b) and (3.16) highlight an important structural feature: the key issue for the evaluation of the SIR distribution is the marginalization of the conditional characteristic function (or Laplace transform) of the aggregate interference, i.e., $\psi_{\mathsf{i}_{j,k}|\mathbf{x}_k}(\cdot)$ (or $\mathcal{L}_{\mathsf{i}_{j,k}|\mathbf{x}_k}(\cdot)$), over the distribution of the receiver location $\mathbf{x}_k$.

Maximum SIR Legitimate Receiver

Based on the results shown in Section 3.4.1, the following three results (i.e., Theorem 2, Corollaries 2 and 3) are provided to obtain the CDF of the SIR when the maximum SIR receiver selection strategy is adopted by transmitters. Three different network scenarios will be taken into account. In particular, Theorem 2 concerns the analysis of the FIN, Corollary 2 analyzes the FHN as a special case of the FIN and recalls results from [76], while Corollary 3 gives a formulation for PINs. Furthermore, Case Study 1 is presented to provide insights from our findings and validate the analysis.

Consider an LT in $\boldsymbol{x}_j$ and all the LRs with index set $\mathcal{R}_j$ in a bounded set $\mathcal{A}_{\mathcal{R}_j} \subset \mathbb{R}^d$. The location of the maximum SIR receiver is defined as $\mathbf{x}_{\breve{k}} \in \Pi_{\mathrm{rx}}$ where $\breve{k} \triangleq \arg\max_{k\in\mathcal{R}_j}\{\mathsf{z}_{j,k}\}$.

Theorem 2 (*FIN: maximum SIR receiver*) *Let the LTN and the LRN be described by the IPPPs Π_{tx} and Π_{rx} with intensity functions $\lambda_{\mathrm{tx}}(\boldsymbol{x})$ and $\lambda_{\mathrm{rx}}(\boldsymbol{x})$, respectively. The CDF of the SIR at $\mathbf{x}_{\breve{k}}$ when $\boldsymbol{x}_j$ is the useful transmitter, i.e., $\mathsf{z}_{j,\breve{k}} \triangleq \max_{k\in\mathcal{R}_j}\{\mathsf{z}_{j,k}\}$, is given by*

$$F_{\mathsf{z}_{j,\breve{k}}}(z) = \exp\left\{\left(F_{\mathsf{z}_{j,k}}(z) - 1\right)\Lambda_{\mathrm{rx}}(\mathcal{A}_{\mathcal{R}_j})\right\} \tag{3.18}$$

where $F_{\mathsf{z}_{j,k}}(z)$ is the CDF of the SIR of a generic link obtained by Lemma 1 or 2.

Proof 5 *The proof is given in Appendix B.1.* □

Corollary 2 (*FHN: maximum SIR receiver*) *Let the LTN and the LRN be described by the HPPPs Π_{tx} and Π_{rx} in $\mathcal{A} \subseteq \mathbb{R}^2$ with intensities λ_{tx} and λ_{rx}, respectively. Let $\mathcal{A}_{\mathcal{R}_j}$ be a circular region centered in $\boldsymbol{x}_j$ with radius r_{M} in which the LRs are located. The CDF of $\mathsf{z}_{j,\breve{k}}$ is given by (3.18) with*

$\Lambda_{\rm rx}(\mathcal{A}_{\mathcal{R}_j}) = \pi r_{\rm M}^2 \lambda_{\rm rx}$, *where* $F_{\mathsf{z}_{j,k}}(z)$ *is defined in (3.14a)-(3.15),* $\mathsf{i}_{j,k}$ *is a skewed stable RV with a characteristic function given by (3.10b), and* $\mathsf{r}_{j,k}^2 \sim \mathcal{U}(0, r_{\rm M}^2]$.

Proof 6 *The proof is given in Appendix B.2.* □

Note that Corollary 2 summarizes what is analyzed in Section IV-A2 of [76] as a special case of Theorem 2.

Corollary 3 (*PIN: maximum SIR receiver*) *Let the LTN and the LRN be described by the IPPP* $\Pi_{\rm tx}$ *with intensity function* $\lambda_{\rm tx}(\boldsymbol{x})$, *and the HPPP* $\Pi_{\rm rx}$ *with intensity* $\lambda_{\rm rx}$, *respectively. The CDF of* $\mathsf{z}_{j,\check{k}}$ *is given by (3.18) with* $\Lambda_{\rm rx}(\mathcal{A}_{\mathcal{R}_j}) = \pi r_{\rm M}^2 \lambda_{\rm rx}$, *where* $F_{\mathsf{z}_{j,k}}(z)$ *is obtained by (3.14a)-(3.15) and*

$$\psi_{\mathsf{g}_{j,k}}(\jmath\omega) = \psi_{\mathsf{h}_{j,k}}(\jmath\omega) \times \mathbb{E}_{\mathsf{r}_{j,k}} \mathbb{E}_{\theta_{j,k}} \big\{ \psi_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\theta_{j,k}} \left(-\jmath\omega \mathsf{r}_{j,k}^{2b} z \right) \big\} \tag{3.19}$$

$\psi_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\theta_{j,k}}(\jmath\omega)$ *is given by (3.9),* $\mathsf{r}_{j,k}^2 \sim \mathcal{U}(0, r_{\rm M}^2]$, *and* $\theta_{j,k} \sim \mathcal{U}(0, 2\pi]$.

Proof 7 *The proof is given in Appendix B.3.* □

Case Study 1 *Consider the PIN setting of Corollary 3, in a Nakagami-m fading environment with average channel power* $\overline{\Omega}$. *Further, consider for the LTN a Gaussian*[6] *intensity function centered in the origin of a coordinate system (see Fig. 3.2) with variance* σ^2 *on each axis, i.e.,*

$$\lambda_{\rm tx}(\boldsymbol{x}) = \frac{\Lambda_{\rm tx}(\mathcal{A})}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}} \,. \tag{3.20}$$

The CDF of $\mathsf{z}_{j,\check{k}}$ *is given by (3.18) with* $\Lambda_{\rm rx}(\mathcal{A}_{\mathcal{R}_j}) = \pi r_{\rm M}^2 \lambda_{\rm rx}$, *where*

$$F_{\mathsf{z}_{j,k}}(z) = 1 - \sum_{i=0}^{m-1} \frac{(-1)^i}{i!} \times \left[\frac{d^{(i)}}{ds^i} \mathbb{E}_{\mathsf{r}_{j,k}} \mathbb{E}_{\theta_{j,k}} \left\{ \mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\theta_{j,k}} \left(s\, m \mathsf{r}_{j,k}^{2b} z \right) \right\} \right]_{s=1} \tag{3.21}$$

$\mathcal{L}_{\mathsf{i}_{j,k}|\mathsf{r}_{j,k},\theta_{j,k}}\big(s\, m r_{j,k}^{2b} z\big)$ *is found to be expressed as (3.22),* $\mathsf{r}_{j,k}^2 \sim \mathcal{U}(0, r_{\rm M}^2]$, *and* $\theta_{j,k} \sim \mathcal{U}(0, 2\pi]$.

Proof 8 *Case Study 1 is a special case of Corollary 3 with Gaussian intensity function and Nakagami-m fading. The derivation of (3.21) is straightforward considering Lemma 2 instead of Lemma 1. To obtain (3.22), (3.9) is rearranged taking into account (3.17), (3.20), and the Laplace transform of the square channel gain in Nakagami-m fading, i.e.,* $\mathcal{L}_{\mathsf{h}}(s) = \left(\frac{m}{\overline{\Omega} s + m}\right)^m$. □

[6]This intensity function can be interpreted as a bivariate Gaussian PDF with same variance on the two jointly Gaussian components (see [191]), weighted by $\Lambda_{\rm tx}(\mathcal{A})$.

k^{th} Closest Receiver

Consider all the selectable LRs $k = 1, 2, \ldots, \mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}$ of the transmitter $\boldsymbol{x}_j$. Consider the orderly index set of the LRs $\{(k)\}$ where the ordering is based on distances, i.e., $\mathsf{r}_{j,(k)} \leq \mathsf{r}_{j,(k+1)}$ for all k. When the k^{th} closest LR is selected, i.e., $\bar{k} = (k)$, the following result holds.

Theorem 3 (*FIN: k^{th} closest receiver*) *In the FIN setting of Theorem 2, the CDF of the SIR between $\boldsymbol{x}_j$ and its k^{th} closest receiver $\mathsf{x}_{(k)}$, i.e., $\mathsf{z}_{j,(k)}$, is given by (3.14a) and (3.14b) with $k = (k)$,[7] and*

$$\psi_{\mathsf{g}_{j,(k)}}(\jmath\omega) = \psi_{\mathsf{h}_{j,(k)}}(\jmath\omega) \times \mathbb{E}_{\mathsf{r}_{j,(k)}}\Big\{\mathbb{E}_{\boldsymbol{\theta}_{j,(k)}|\mathsf{r}_{j,(k)}}\Big\{\psi_{\mathsf{i}_{j,(k)}|\mathsf{r}_{j,(k)},\boldsymbol{\theta}_{j,(k)}}\big(-\jmath\omega r_{j,(k)}^{2b} z\big)\Big\}\Big\} \quad (3.23)$$

where $\psi_{\mathsf{i}_{j,(k)}|\mathsf{r}_{j,(k)},\boldsymbol{\theta}_{j,(k)}}(\jmath\omega)$ is given by (3.9) with $k = (k)$. The distributions of $\mathsf{r}_{j,(k)}$ ad $\boldsymbol{\theta}_{j,(k)}$ are derived in Appendix B.4.

Proof 9 *Consider the framework of Lemma 1 with $k = (k)$ in (3.14a)-(3.14b). Before carrying out the expectation of (3.14b), let us emphasize that $\mathsf{r}_{j,(k)}$ and $\boldsymbol{\theta}_{j,(k)}$ are dependent RVs. In fact, if the LRs are inhomogeneous, for a certain value of the distance $\overline{r}_{j,(k)}$, there exists an angular direction $\overline{\theta}_{j,(k)}$ in which the probability of finding the k^{th} closest receiver is maximized*

$$\overline{\theta}_{j,(k)} = \underset{\theta \in \mathcal{C}_{j,(k)}}{\operatorname{argmax}}\, \lambda_{\text{rx}}\left(\overline{r}_{j,(k)}, \theta\right) \quad (3.24)$$

where $\mathcal{C}_{j,(k)}$ is the the circumference with center $\boldsymbol{x}_j$ and radius $\overline{r}_{j,(k)}$. Considering $k = (k)$, (3.14b) can be rearranged by the chain rule of conditional expectation to obtain (3.23); then (3.9) is plugged in with (k) in place of k. □

Corollary 4 (*FHN: k^{th} closest receiver*) *In the FHN setting of Corollary 2, the CDF of $\mathsf{z}_{j,(k)}$ is given by (3.14a)-(3.14b) where $k = (k)$, $\mathsf{i}_{j,(k)}$ is a skewed stable RV with characteristic function given by (3.10b) except for the replacement $k = (k)$, and $\mathsf{r}_{j,(k)}^2$ is an Erlang distributed RV [192–194] with characteristic function given by*

$$\psi_{\mathsf{r}_{j,(k)}^2}(\jmath\omega) = \left(1 - \frac{\jmath\omega}{\pi\lambda_{\text{rx}}}\right)^{-k}. \quad (3.25)$$

[7] From here on and for the rest of the subsection, whenever we refer to an equation involving the index k of a generic receiver, the reader should substitute it with (k) for the case of the k^{th} closest receiver.

Proof 10 *Consider (3.14b) with $k = (k)$. Since transmitter and receiver locations are modeled according to HPPPs over the set $\mathcal{A}$, the aggregate interference characteristic function is given by (3.10b) where $k = (k)$. Further, the squared distance $\mathsf{r}^2_{j,(k)}$ between $\boldsymbol{x}_j$ and its k^{th} closest receiver $\mathbf{x}_{(k)}$ is an Erlang RV with characteristic function defined in (3.25).* □

Note that the case analyzed in Section IV-A1 of [76] undergoes to the same hypotheses of Corollary 4 and can be considered as a special case of Theorem 3.

Corollary 5 (*PIN:* k^{th} *closest receiver*) *In the PIN setting of Corollary 3, the CDF of $\mathsf{z}_{j,(k)}$ is given by (3.9), (3.14a), and (3.19) with $k = (k)$; where $\mathsf{r}^2_{j,(k)}$ is Erlang distributed with characteristic function defined in (3.25); and $\theta_{j,(k)} \sim \mathcal{U}(0, 2\pi]$.*

Proof 11 *The proof directly follows from the one of Corollary 3 with $k = (k)$ and by considering the Erlang distribution for the square distance $\mathsf{r}^2_{j,(k)}$.* □

Case Study 2 *Consider the assumptions made in Case Study 1. The CDF of $\mathsf{z}_{j,(k)}$ is given by*

$$F_{\mathsf{z}_{j,(k)}}(z) = 1 - \sum_{i=0}^{m-1} \frac{(-1)^i}{i!} \times \left[\frac{d^{(i)}}{ds^i} \mathbb{E}_{\mathsf{r}_{j,(k)}} \mathbb{E}_{\theta_{j,(k)}} \left\{ \mathcal{L}_{\mathsf{i}_{j,(k)}|\mathsf{r}_{j,(k)},\theta_{j,(k)}} \left(s\, m r^{2b}_{j,(k)} z \right) \right\} \right]_{s=1} \tag{3.26}$$

where $\mathcal{L}_{\mathsf{i}_{j,(k)}|\mathsf{r}_{j,(k)},\theta_{j,(k)}}\left(s\, m r^{2b}_{j,(k)} z\right)$ is obtained in (3.22) with $k = (k)$; $\mathsf{r}^2_{j,(k)}$ is an Erlang distributed RV with characteristic function defined in (3.25); and $\theta_{j,(k)} \sim \mathcal{U}(0, 2\pi]$

Proof 12 *Case Study 2 is a special case of Corollary 5 with Gaussian intensity function and Nakagami-m fading. The derivation of (3.26) is straightforward considering Lemma 2 instead of Lemma 1.* □

3.4.2 SIR in the Eavesdropping Network

The framework for the characterization of the SIR in the eavesdropping network is the same as defined for the legitimate network. The main difference comes from the assumption of considering a population of IIs that help the legitimate network in keeping the information confidential. In particular, IIs know the positions of LRs and have the capability of nulling the transmission

power sent in the directions of such receivers, effectively deteriorating only the reception of the ERN. Specifically, either IIs are equipped with multiple antennas, and, hence, can perform null-steering beamforming or interference alignment [110] at the LRs' locations, or IIs with a single antenna cooperate to mimic multiantenna jammers [73].

In Section 3.7, we also show scenarios in which IIs are inactive and, hence, the eavesdropping channels are as much impaired as the legitimate ones. Practical techniques to impair eavesdropping channels can be found in [73, 75, 109, 110, 169–175]. All results of Section 3.4.1 hold also for the eavesdropping link, where the interferers of the ERN are modeled by the PPP Π_{ie} given by the superposition of Π_{tx} and Π_{jx} with intensity function $\lambda_{\text{ie}}(\boldsymbol{x}) = \lambda_{\text{jx}}(\boldsymbol{x}) + \lambda_{\text{tx}}(\boldsymbol{x})$ for all $\boldsymbol{x} \in \mathcal{A} \subseteq \mathbb{R}^d$. The eavesdropping link consists of the transmitter at $\boldsymbol{x}_j$ and the receiver at $\mathbf{x}_i \in \Pi_{\text{ex}}$. Recall that secrecy performance is determined by the ER with maximum SIR. The results of Section 3.4.1 are used, with ER index $\breve{l} \in \mathcal{E}_j$ s.t. $\mathsf{z}_{j,\breve{l}} \triangleq \max\limits_{i \in \mathcal{E}_j} \{\mathsf{z}_{j,l}\}$ in place of the selected receiver with index $\breve{k}$.

3.5 Network Secrecy Metrics

Based on the framework developed in Section 3.4 for received SIR characterization, this section defines the secrecy metrics for inhomogeneous networks. Among different locations of the network, the aggregate interference can dramatically change, depending on the panorama of interferers at the considered point. Hence, we first introduce local secrecy metric, then we define global metrics to summarize the overall network performance.

3.5.1 Maximum Secrecy Rate

In Section III-A of [76], the maximum secrecy rate (MSR) of a Gaussian wireless-tap channel is extended to scenarios with interference generated by a homogeneous network, when receivers treat interference as noise. Recall the conditional MSR $\varphi_{j,\bar{k},\breve{l}}$, which is the maximum transmission rate that a transmitter can employ remaining in the condition of perfect secrecy [70,164]. The MSR of the link consisting of the LT, the selected LR and the ER at $\boldsymbol{x}_j$, $\boldsymbol{x}_{\bar{k}}$, and $\boldsymbol{x}_{\breve{\imath}}$, respectively, is determined by the most capable ER (i.e., the one with highest SIR) with index $\breve{l} \triangleq \arg\max\limits_{i \in \mathcal{E}_j} \{\mathsf{z}_{j,l}\}$. The conditional MSR is given by

$$\varphi_{j,\bar{k},\breve{l}} = \left[c(\mathsf{z}_{j,\bar{k}}) - c(\mathsf{z}_{j,\breve{l}}) \right]^+ \tag{3.27}$$

and it is is measured in confidential information bits per second per Hertz, i.e., [cib/s/Hz] (c.f. [76]), where $c(z) \triangleq \log_2(1+z)$ [bit/s/Hz] is the capacity of the Gaussian wireless-tap channel, $\mathsf{z}_{j,\bar{k}}$ is the SIR at the selected receiver, and $\mathsf{z}_{j,\check{l}}$ is the SIR at the ER with maximum SIR. Hence, the local maximum secrecy rate (LMSR) is defined as the average MSR of a link originated in $\boldsymbol{x}_j$ over channel gains and point configurations, i.e.,

$$R_j \triangleq \mathbb{E}^{!j}\{\mathsf{\varphi}_{j,\bar{k},\check{l}}\}\,. \tag{3.28}$$

where $\mathbb{E}^{!j}\{\cdot\}$ is the reduced Palm expectation conditional on the intended transmitter at $\boldsymbol{x}_j$, i.e., the expectation over all point configurations having the intended transmitter at $\boldsymbol{x}_j$ with its removal from the point sequence (c.f. [189]).Consider $\mathsf{z}_{j,\bar{k}}$ and $\mathsf{z}_{j,\check{l}}$ to be independent.[8] The expectation of (3.28) is computed over SIRs as

$$R_j = \int_0^\infty c(z_2) F_{\mathsf{z}_{j,\check{l}}}(z_2) f_{\mathsf{z}_{j,\bar{k}}}(z_2) dz_2 - \int_0^\infty \int_0^{z_2} c(z_1) f_{\mathsf{z}_{j,\check{l}}}(z_1) f_{\mathsf{z}_{j,\bar{k}}}(z_2) dz_1 dz_2\,. \tag{3.29}$$

Remark 1 *R_j expresses the average MSR of a link with the LT located in $\boldsymbol{x}_j$. Hence, it is a metric that describes secrecy performance from the single link point of view and is particularly useful for link design.*

It is also worth defining a metric to describe the secrecy performance from the network point of view. The local network secrecy rate density (LNSRD) is defined as

$$\rho_j(\boldsymbol{x}_j) \triangleq \lambda_{\text{tx}}(\boldsymbol{x}_j) R_j \tag{3.30}$$

for all $\mathsf{x}_j \in \mathcal{A}$ and measured in [cib/s/Hz/m^2]. Note that such a metric is a density, being weighted for the density of transmitters in $\boldsymbol{x}_j$, and describe the performance in terms of secrecy rate per unit area. The definition of $\rho_j(\boldsymbol{x}_j)$ highlights that a high level of information confidentiality can be achieved in a certain region not only if every single link has a high MSR, but also if that region is densely populated by links with low MSR values. To describe the overall network performance, we define a global secrecy metric that takes into account all the possible locations of the LT $\boldsymbol{x}_j$. For that purpose, consider

[8] The approximation that neglect the spatial correlation of the interference has been shown to be good in [76] (see Fig. 3)

the spatial average of R_j as

$$\overline{R} \triangleq \int_{\mathcal{A}} R_j(\boldsymbol{x}) f^{\mathrm{tx}}_{\mathbf{x}_j}(\boldsymbol{x}) d\boldsymbol{x} \tag{3.31a}$$

$$= \frac{1}{\Lambda_{\mathrm{tx}}(\mathcal{A})} \int_{\mathcal{A}} \rho_j(\boldsymbol{x}) d\boldsymbol{x} \tag{3.31b}$$

$$= \frac{1}{\Lambda_{\mathrm{tx}}(\mathcal{A})} R_{\mathrm{ns}} \tag{3.31c}$$

where $f^{\mathrm{tx}}_{\mathbf{x}_j}(\boldsymbol{x}) = \lambda_{\mathrm{tx}}(\boldsymbol{x})/\Lambda_{\mathrm{tx}}(\mathcal{A})$ and (3.30) are used to obtain (3.31b). Then, (3.31b) is used together with (3.31c) to define the network secrecy rate (NSR)[9] as

$$R_{\mathrm{ns}} \triangleq \int_{\mathcal{A}} \rho_j(\boldsymbol{x}) d\boldsymbol{x} \,. \tag{3.32}$$

Remark 2 *Differently from R_j, that is related to a single link, R_{ns} is related to all the links in the set $\mathcal{A}$ and represents the total secrecy rate over $\mathcal{A}$. Moreover, $\rho_j(\boldsymbol{x}_j)$ is the pointwise density associated with R_{ns}.*

3.5.2 Secrecy Throughput Density

Consider that an LT cannot achieve the MSR unless it knows the SIRs at the selected receiver and at each ER. It is worth introducing a metric that characterizes the confidential information flowing through legitimate links, which is blind w.r.t. the instantaneous ERs' positions and channels (only stochastic information is assumed). In Sections III-D and III-E of [76], the network secrecy throughput density is defined. We now generalize such a metric to account for the inhomogeneous distribution of nodes.

Consider a desired rate of confidential information R_{s} and a maximum tolerable secrecy outage probability (SOP) $P^{\star}_{\mathrm{so}}$. The LT in $\boldsymbol{x}_j$ transmits the confidential information only if the SIR at the selected receiver is greater than a threshold μ, namely the secrecy protection ratio. Such an event happens with probability $P_{\mathrm{it},j}(\mu) \triangleq \mathbb{P}\left\{\mathsf{z}_{j,\bar{k}} > \mu\right\}$. The secrecy outage event

[9]The NSR is measured in confidential information bits per second per Hertz, i.e., [cib/s/Hz] (c.f. [76]).

is characterized by the SOP

$$P_{\mathrm{so},j}(R_{\mathrm{s}},\mu) \triangleq \mathbb{P}\left\{c(\mathsf{z}_{j,\check{l}}) > c(\mathsf{z}_{j,\bar{k}}) - R_{\mathrm{s}} | \mathsf{z}_{j,\bar{k}} > \mu\right\} \tag{3.33a}$$

$$= \frac{1}{1-F_{\mathsf{z}_{j,\bar{k}}}(\mu)} \tag{3.33b}$$

$$\times \Big[F_{\mathsf{z}_{j,\bar{k}}}(\mu) F_{\mathsf{z}_{j,\check{l}}}(\frac{\mu+1}{2^{R_{\mathrm{s}}}}-1) - F_{\mathsf{z}_{j,\bar{k}}}(\mu) \tag{3.33c}$$

$$+ \int_{\frac{\mu+1}{2^{R_{\mathrm{s}}}+1}}^{\infty} F_{\mathsf{z}_{j,\bar{k}}}(2^{R_{\mathrm{s}}}(1+y)-1) f_{\mathsf{z}_{j,\check{l}}}(y) dy\Big] \tag{3.33d}$$

which is obtained by the Bayes rule. Hence, the secrecy protection ratio of the network is set as the most conservative value over the possible transmitter location $\boldsymbol{x}_j$ that maximize $P_{\mathrm{it},j}(\mu)$ with the constraint $P_{\mathrm{so},j}(R_{\mathrm{s}},\mu) \leq P_{\mathrm{so}}^{\star}$, i.e.,

$$\mu^{\star} = \max_{\boldsymbol{x}_j \in \mathcal{A}} \Big\{ \arg\max_{\mu \in \mathcal{M}^j} P_{\mathrm{it},j}(\mu) \Big\} \tag{3.34}$$

which is solved by exhaustive search where $\mathcal{M}^j = \{\mu : P_{\mathrm{so},j}(R_{\mathrm{s}},\mu) \leq P_{\mathrm{so}}^{\star}\}$. We then define the *local secrecy throughput* (LST) as

$$T_j \triangleq \mathbb{E}^{!j} \mathbb{1}_{[\mu^{\star},\infty)}(\mathsf{z}_{j,\bar{k}}) R_{\mathrm{s}} \tag{3.35}$$

that is the average secrecy throughput for a link with the LT located at $\boldsymbol{x}_j$. Then, T_j is determined as

$$T_j = P_{\mathrm{it},j}(\mu^{\star}) R_{\mathrm{s}} \,. \tag{3.36}$$

To describe the secrecy throughput flowing in the network we define the local network secrecy throughput density (LNSTD) by

$$\tau_j(\boldsymbol{x}_j) \triangleq \lambda_{\mathrm{tx}}(\boldsymbol{x}_j) T_j \,. \tag{3.37}$$

Furthermore, in analogy to the NSR, we define the network secrecy throughput (NST) to describe the overall network performance in terms of total secrecy throughput over a certain area $\mathcal{A}$ as

$$T_{\mathrm{ns}} = \int_{\mathcal{A}} \tau_j(\boldsymbol{x}) d\boldsymbol{x} \,. \tag{3.38}$$

Remark 3 *Note that local secrecy metrics R_j, T_j, $\rho_j(\boldsymbol{x}_j)$, and $\tau_j(\boldsymbol{x}_j)$ are defined pointwise and describe a surface for all $\boldsymbol{x}_j \in \mathcal{A}$. Global secrecy metrics like R_{ns} and T_{ns} condense the information provided by local metrics in a single value that is proportional to the spatial means of R_j and T_j, respectively.*

Remark 4 *Eq. (3.30) and (3.37) show that spatial variability of LNSRD and LNSTD are mainly caused by two different elements: 1) direct dependency from* $\lambda_{\text{tx}}(\boldsymbol{x}_j)$*, and 2) implicit dependency from intensity functions* $\lambda_{\text{tx}}(\boldsymbol{x})$*,* $\lambda_{\text{rx}}(\boldsymbol{x})$*,* $\lambda_{\text{jx}}(\boldsymbol{x})$*, and* $\lambda_{\text{ex}}(\boldsymbol{x})$*. Such an implicit dependency is due to the SIRs* $\mathsf{z}_{j,\bar{k}}$ *and* $\mathsf{z}_{j,\check{l}}$*, which themselves depend on the point process of the LRs, the point process of ERs, and that of the IIs.*

3.6 Case Studies

Sections 3.3, 3.4, and 3.5 show the influence of intrinsic network properties, such as aggregate interference and node spatial distribution, on network secrecy. Section 3.2 presents the network model as a superposition of four PPP, where each of those is described by its intensity function. Inhomogeneities in such functions as well as local imbalances between values of different subnetworks heavily affect the local secrecy level. In this section we introduce and analyze some case studies to explore the inhomogeneous network secrecy performance. In particular, Section 3.6.1 presents the *dense-sparse model* to capture the fundamental effect of a rise and a fall of the node intensity compared to a constant level, while Section 3.6.2 introduce several case studies where LTs, LRs, ERs, and IIs follow either the dense-sparse or the homogeneous models.

3.6.1 The Dense-Sparse Model

Consider a generic PPP $\Pi_{\square}$ where $\square = \{\text{tx, rx, jx, ex}\}$. $\Pi_{\square}$ can be either a HPPP or IPPP. For the IPPPs we have considered a Gaussian intensity functions centered in the origin with variance σ^2 on each axis (see Fig. 3.2), hence

$$\lambda_{\square}(\boldsymbol{x}) = \begin{cases} \frac{\Lambda_{\square}(\mathcal{A})}{2\pi\sigma^2} e^{-\frac{u^2+v^2}{2\sigma^2}} & \text{if } \Pi_{\square} \text{ is an IPPP} \\ \lambda_{\square} & \text{if } \Pi_{\square} \text{ is a HPPP} \end{cases} . \tag{3.39}$$

For a fair comparison it is necessary that $\mathcal{A}$ and σ^2 are such that

$$\int_{\mathcal{A}} \frac{1}{2\pi\sigma^2} e^{-\frac{u^2+v^2}{2\sigma^2}} \simeq 1 .$$

We define the high density (HD) region by the surface in which the intensity function of the IPPP is greater than $\lambda_{\square}$ and the low density (LD) region by the surface in which such intensity function is smaller than $\lambda_{\square}$ (see Fig. 3.5). The former represents a peak of the node density while the latter

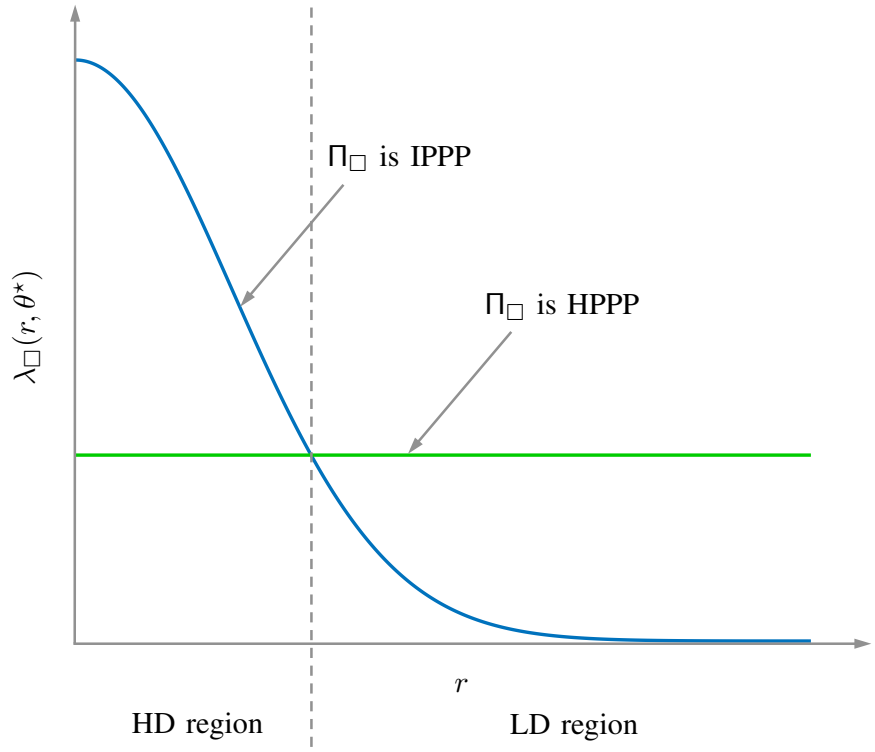

Figure 3.5: Half of a section of the intensity function of an IPPP and HPPP, respectvely. It is divided in the HD and LD region.

represents a hole of the node density. The above defined model is particularly adequate in scenarios where nodes are concentrated in a specific area, and tend to rarefy outside it. This situation can occur in vehicular networks, e.g., at the intersection of two streets in an urban area or at the toll booth on a highway; or in pedestrian networks, e.g., at a concert or at the traffic light in correspondence of a crosswalk; in tactic scenario, e.g., a squadron of drones, and so on so forth. More realistic models can be considered to avoid the total rarefaction of the network. For example a superposition of a dense-sparse model with an homogeneous model can effectively represent a scenario with a high concentration of nodes in a specific area, that decrease to a standard uniform concentration. In such a case, the network can be considered as a superposition of point processes with intensity function composed by two parts, i.e., $\lambda_\square(\boldsymbol{x}) = \lambda_\square^{\text{inh.}}(\boldsymbol{x}) + \lambda_\square^{\text{hom.}}$. All the results of this thesis directly apply to such a scenario.

3.6.2 Network Scenarios

While HPPPs are usually compared on a theoretically infinite surface by means of their intensity (nodes per square meter in a two dimension area), a fair comparison between inhomogeneous PPPs with different intensity functions can be carried out by considering their intensity measures over a bounded region $\mathcal{A}$. Hence we will consider different scenarios where each subnetwork follows the dense-sparse model. Then, we refer the intensity measures of the four subnetworks to that of an HPPP with intensity λ_{h} by

$$\Lambda_{\mathrm{tx}}(\mathcal{A}) = \alpha_1 \Lambda_{\mathrm{h}}(\mathcal{A}) \tag{3.40a}$$

$$\Lambda_{\mathrm{rx}}(\mathcal{A}) = (1-\alpha_1) \Lambda_{\mathrm{h}}(\mathcal{A}) \tag{3.40b}$$

$$\Lambda_{\mathrm{jx}}(\mathcal{A}) = \alpha_2 \Lambda_{\mathrm{h}}(\mathcal{A}) \tag{3.40c}$$

$$\Lambda_{\mathrm{ex}}(\mathcal{A}) = \alpha_3 \Lambda_{\mathrm{h}}(\mathcal{A}) \tag{3.40d}$$

where $\alpha_1, \alpha_2, \alpha_3 \in [0,1]$ and $\Lambda_{\mathrm{h}}(\mathcal{A}) = \lambda_{\mathrm{h}}|\mathcal{A}|$. We now define as case studies six network scenarios where imbalances between the spatial distributions of the LTN, LRN, ERN, and IIN are considered. We introduce some specific terminology to refer to the considered scenarios: the first specification (smart/non smart) refers to the LTN and LRN and the second specification (informed/non informed) to the ERN and IIN. In particular, the terms "smart" and "informed" refers to an inhomogeneous distribution of nodes. The following case studies have been analyzed:

- smart informed (SI): all PPPs are inhomogeneous;
- smart non-informed (SNI): inhomogeneous LTN and LRN, homogeneous ERN and IIN;
- non-smart informed (NSI): homogeneous LTN and LRN, inhomogeneous ERN and IIN;
- non-smart non-informed (NSNI): all PPPs are homogeneous.

In addition, two hybrid scenarios have been considered; they will be referred to as follows:

- hybrid network scenario 1 (HNS1): inhomogeneous LTN and IIN, homogeneous LRN and ERN;
- hybrid network scenario 2 (HNS2): inhomogeneous IIN, homogeneous LTN, LRN, and ERN.

To each of the six settings above, there can be appended the third specification regarding the receiver selection technique: maximum SIR (MS) or k^{th} closest (KC).

3.7 Numerical Results

This section provides results based on the analytical framework developed in Sections 3.3, 3.4, and 3.5. In the first part, the analytical distribution of the SIR at the selected receiver is verified by simulations. In the second part, we explore the spatial behavior of local secrecy metrics and we provide global secrecy metrics' values for different comparative scenarios and network settings.

For IPPPs we have considered Gaussian intensity functions centered in the origin with the same variance σ^2 on each axes. The scattering surface is a disk with maximum radius $R_{\max} = 5\sigma$ (see Fig. 3.2). The LT operates the receiver selection with two different modes: the MS and the KC with $k = 1$.

3.7.1 CDF of the Received SIR

Fig. 3.6 shows the CDF $F_{\mathsf{z}_{j,\check{k}}}(z)$ of the received SIR at the maximum SIR (continuous lines) and at the closest (dashed lines) receiver selected by an LT located at different distances from the origin (different markers correspond to different locations of the LT). A PIN has been considered in a Rayleigh ($m = 1$) fading channel. As expected, higher SIR values are more likely to occur when the maximum SIR receiver is selected. It can be observed that analytical results (lines) and simulations (markers) match almost perfectly.

3.7.2 Secrecy Metrics Analysis

Competitive Scenarios Performance

Fig. 3.7 shows the LMSR R_j as a function of the distance of the LT from the origin, i.e., $\|\boldsymbol{x}_j\|$, for different receiver selection strategies (solid and dashed lines) and different network scenarios (different markers). Let us remind the structure of the conditional MSR of a link in $\boldsymbol{x}_j$ to provide insights

$$\mathsf{\varphi}_{j,\bar{k},\check{l}} = \left[\log\left\{ 1 + \mathsf{h}_{j,\bar{k}} \left[\sum_{\mathbf{x}_q \in \Pi_{\mathrm{ir}}} \mathsf{h}_{q,\bar{k}} \left(\frac{\mathsf{r}_{j,\bar{k}}}{\mathsf{r}_{q,\bar{k}}} \right)^{2b} \right]^{-1} \right\} \right. \\ \left. - \log\left\{ 1 + \mathsf{h}_{j,\check{l}} \left[\sum_{\mathbf{x}_w \in \Pi_{\mathrm{ie}}} \mathsf{h}_{w,\check{l}} \left(\frac{\mathsf{r}_{j,\check{l}}}{\mathsf{r}_{l,\check{l}}} \right)^{2b} \right]^{-1} \right\} \right]^{+}. \quad (3.41)$$

Note the behavior of the HNS1 curve, which shows an imbalance between LTs' (inhomogeneous) and LRs' (homogeneous) distributions. Intuitively, we expect that the high density of LTs and IIs would lead to a high performance

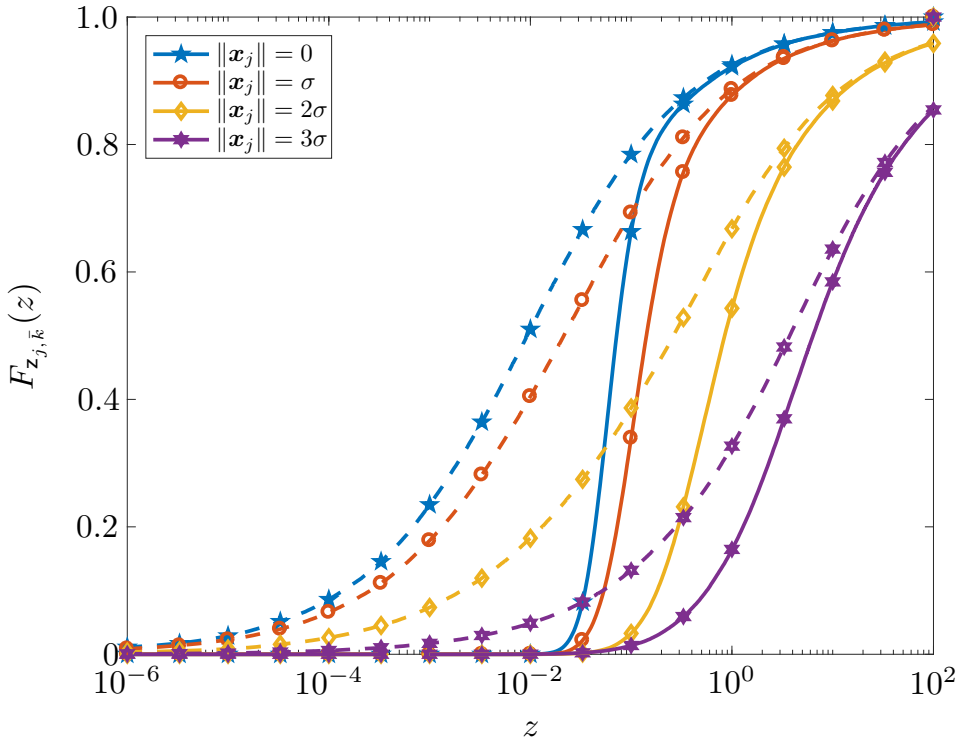

Figure 3.6: Shows $F_{\mathsf{z}_{j,\bar{k}}}(z)$ for different transmitter locations when the closest (dashed lines) and maximum SIR (continuous lines) receiver is selected. A circular region has been considered with $R_{\max} = 15$ [m], $\lambda_{\text{rx}} = 0.5$ [node/m^2], $\Lambda_{\text{tx}}(\mathcal{A}) = \lambda_{\text{rx}}\pi R_{\max}^2$, $\sigma^2 = 3$ [m^2], $m = 1$, $b = 2$, $\overline{\Omega} = 1$.

in the HD region, which is not verified. This can be attributed to the fact that both the path loss and the aggregate interference heavily impair the legitimate channel ($\mathsf{r}_{q,\bar{k}}$ for all $\mathbf{x}_q \in \Pi_{\text{ir}}$, i.e., the distances between interferers and the selected raceiver by $\boldsymbol{x}_j$, are much lower than $\mathsf{r}_{j,\bar{k}}$ on average) and, also, the performance in terms of achievable secrecy rate of the link. The performance improves for increasing $\|\boldsymbol{x}_j\|$ because the interference level decreases, i.e., $\mathsf{r}_{q,\bar{k}}$ for all $\mathbf{x}_q \in \Pi_{\text{ir}}$ increase on average with the increase of $\|\boldsymbol{x}_j\|$.

The performance of other scenarios is characterized by the balance between LTs' and LRs' densities. In the HD region, the NSI curve shows the high density of ERs (low $\mathsf{r}_{j,\check{l}}$ and, hence, low path loss), the SI (full inhomogeneous scenario) overlaps with the NSNI (full homogeneous scenario), and the SNI overlaps with the HNS2, exhibiting the best performance.

In the LD region, the NSI curve shows the low density of ERs (high $\mathsf{r}_{j,\check{l}}$

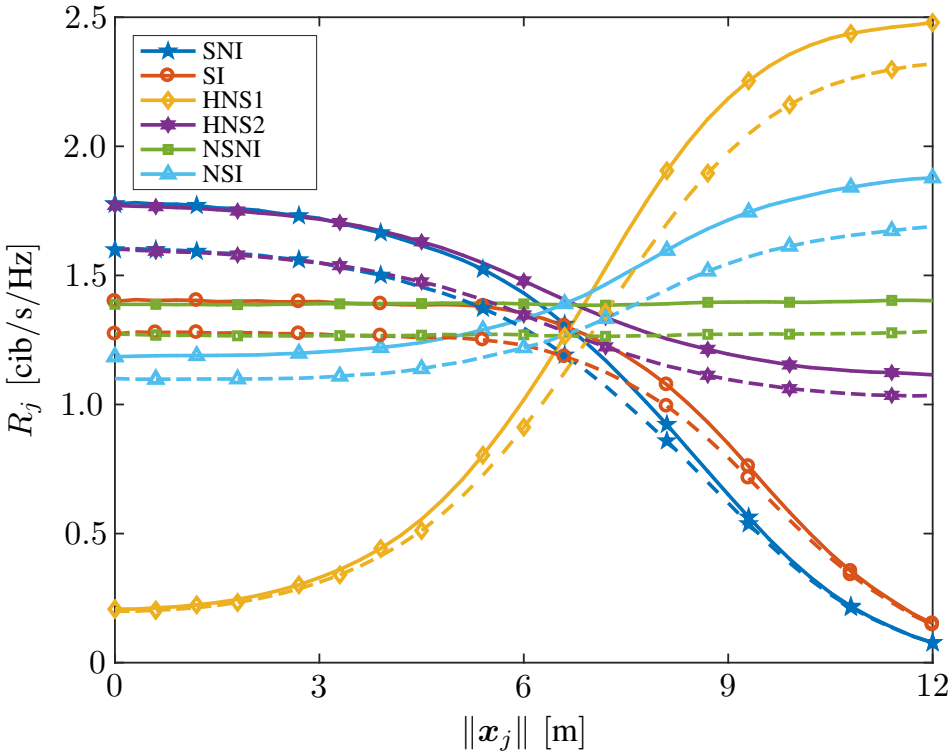

Figure 3.7: LMSR as a function of the location of the LT (distance from the origin $\|\boldsymbol{x}_j\|$). We consider a circular region $\mathcal{A}$, in which Gaussian intensity functions of IPPPs are centered. It has been assumed $R_{\max} = 15$ [m], $|\mathcal{A}| \simeq 706$ [m^2], $\sigma = 3$ [m], $\alpha_1 = \alpha_2 = \alpha_3 = 0.5$, $\lambda_{\mathrm{h}} = 1$ node/m^2, Rayleigh fading ($m = 1$), $b = 2$.

and, hence, high path loss), while the SI's and SNI's performance decays dramatically with the average of the internode distance between source and destination of the legitimate link, i.e., $\mathsf{r}_{j,\bar{k}}$ (inhomogeneous LRN), the NSNI's and HNS2's performance exhibit a floor (the LRN is homogeneous, hence $\mathsf{r}_{j,\bar{k}}$ does not increase arbitrarily, and the effect of path loss is limited).

It is worth noting the causes of the overlapping in the HD region of the SI and SNI curves with the NSNI and HNS2 curves, respectively, which is summarized in the following remark.

Remark 5 *If the receivers and interferers have the same spatial distribution, the channel capacities of every links in the HD region are constant on average.*

The key assumption is that, in the HD region, LTs tends to select nearby LRs, and hence the distribution of nodes seen from those two points is almost

Table 3.2: NSR [cib/s/Hz] values in Fig. 6.

Scenario	MS selection	KC selection
SI	3080.1	2806.2
SNI	3775.5	3401.7
NSI	816.3	743.1
NSNI	787.1	718.1
HNS1	813.2	757.2
HNS2	824.6	750

the same. Consider the legitimate link without any loss of generality; we can approximate the aggregate interference with its maximum component, i.e.,

$$\sum_{\mathsf{x}_q \in \Pi_{\mathrm{ir}}} \frac{\mathsf{h}_{q,\bar{k}}}{\mathsf{r}_{q,\bar{k}}^{2b}} \simeq \frac{\mathsf{h}_{q^\star,\bar{k}}}{\mathsf{r}_{q^\star,\bar{k}}^{2b}} \tag{3.42}$$

where $\mathsf{x}_{q^\star} \in \Pi_{\mathrm{ir}}$ is the index of the interferer with the highest power; hence, the SIR of the legitimate link would depend on average by the ratio $\mathsf{r}_{j,\bar{k}}/\mathsf{r}_{q^\star,\bar{k}}$, which mostly depends on the imbalances between the interferers' and receivers' panoramas seen from $\boldsymbol{x}_j$. A similar behavior can be expected for the eavesdropping link.

Remark 6 *In the HD region, the LMSR for a full inhomogeneous network with equal spatial distributions of the four subnetworks can be approximated by the one of a full homogeneous network.*

Fig. 3.8 shows the LNSRD $\rho_j(\boldsymbol{x}_j)$ as a function of the distance from the origin $\|\boldsymbol{x}_j\|$ for different receiver selection strategies and different comparative scenarios. The curves come from weighting R_j by $\lambda_{\mathrm{tx}}(\boldsymbol{x}_j)$. Hence, in the HD region, a low performance of the single link (low LMSR) can result in an acceptable performance from the network point of view (high LNSRD). This can be justified by the accumulative performance of high density links with non-zero secrecy rate, which leads to a high LNSRD (see HNS1 curves in Fig. 3.7 and Fig. 3.8).

The highest result in terms of NSR (see Table 3.2) is obtained when all the legitimate nodes are inhomogeneous (SNI and SI). In such scenarios, the high density of legitimate links (inhomogeneous LTN) carries a multitude of contribution to the NSR; besides that each contribution is high due to the high availability of receivers (inhomogeneous LRN), which allows each transmitter to select a receiver with a highly reliable channel. In particular a

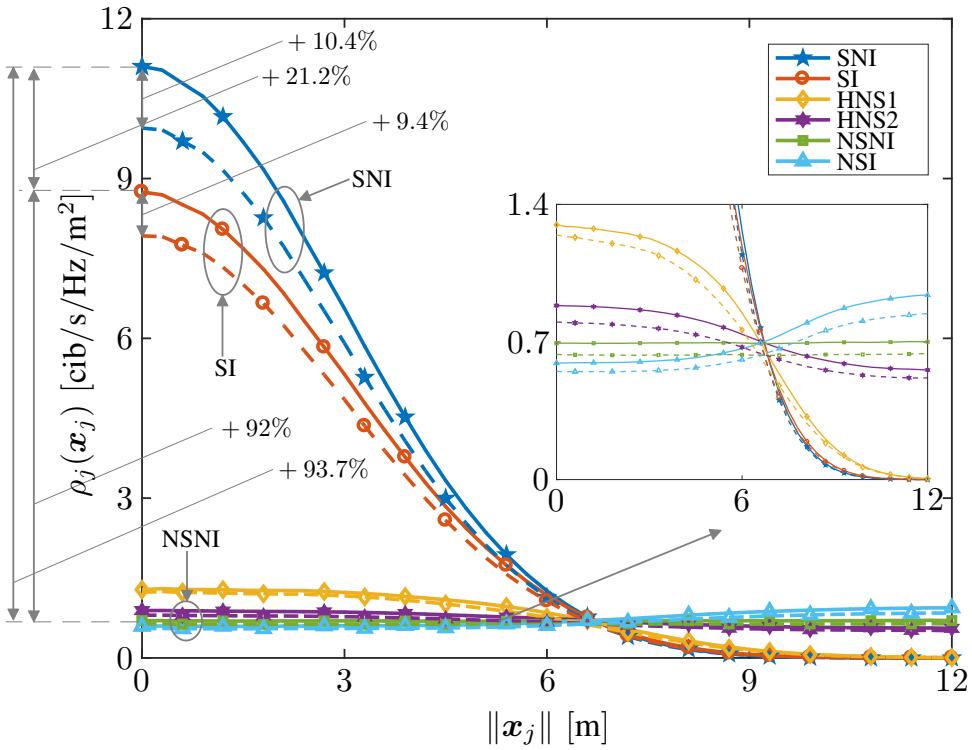

Figure 3.8: LNSRDas a function of the location of the LT (distance from the origin $\|\boldsymbol{x}_j\|$). We consider a circular region $\mathcal{A}$, in which Gaussian intensity functions of IPPPs are centered. It has been assumed $R_{\max} = 15$ [m], $|\mathcal{A}| \simeq 706$ [m^2], $\sigma = 3$ [m], $\alpha_1 = \alpha_2 = \alpha_3 = 0.5$, $\lambda_{\rm h} = 1$ [node/m^2], Rayleigh fading ($m = 1$), $b = 2$.

NSR of 3775.5 and 3080.1 [cib/s/Hz] is obtained on the area $|\mathcal{A}| \simeq 706$ [m^2] in the SNI and SI scenarios, respectively.

Remark 7 *The availability of LRs in dense regions is a key enabler for confidential communications. When a practical ubiquitous eavesdropping channel impairment is difficult to achieve, the transmission of the information on highly reliable channel allows to hide a higher confidential information rate within the total rate. Hence, smart secure destination selection (single-hop networks) and routing (multi-hop networks) are particularly suitable to achieve confidentiality in highly populated networks.*

Furthermore, the selection of the receiver with maximum SIR instead of the $k^{\rm th}$ closest implies higher confidentiality, especially in more dense regions.

For instance the MS selection allows to gain 373.8 [cib/s/Hz] of NSR compared to the KC selection in the SNI scenario (see Table 3.2). Note also that in the SI and SNI settings the decay of performance in LD region is faster compared to the other settings (HNS1, HNS2, and NSNI). HNS2 and NSNI scenarios guarantee a performance floor, thanks to the homogeneity of the LRN.

Table 3.2 shows NSR values obtained by integrating numerically (3.32) for the comparative scenarios. By comparing the NSR values of the smart scenarios (SI and SNI) with the others, and in particular with the one of the full homogeneous scenario (NSNI); a remarkable performance gap can be noticed.

Remark 8 *Even though the inhomogeneous network may show poor performance locally, it can highly outperform the homogeneous network with same measures* $\Lambda_{\square}(\mathcal{A})$ *for* $\square = \{\text{tx, rx, jx, ex}\}$ *in terms of the global network secrecy.*

Variability of Spatial Distributions

Fig. 3.9 shows the network secrecy rate density $\rho_j(\boldsymbol{x}_j)$ as a function of the distance from the origin $\|\boldsymbol{x}_j\|$ in the SI-MS scenario, for different values of the variance of intensity functions of the inhomogeneous point processes describing the various subnetworks, and with non-active IIs, i.e., $\Lambda_{\text{jx}}(\mathcal{A}) = 0$. It can be observed that node concentration highly influences the achievable secrecy performance in terms of secrecy rate per square meter.

Fig. 3.10 shows the network secrecy throughput density $\tau_j(\boldsymbol{x}_j)$ as a function of the distance from the origin $\|\boldsymbol{x}_j\|$ in the SI-MS scenario, for different values of the ratios α_2 and α_3 defined in (3.40c) and (3.40d), respectively. Three cases are compared: the first (blue stars) shows the performance for a low mean number of ERs while IIs are not active; the second (red circles) highlights the performance loss when the mean number of ER increases; and the third (yellow diamonds) shows the performance improvement obtained with IIs having the same intensity measure as the ERs.

3.8 Final Remarks

This chapter develops a framework for design and analysis of inhomogeneous wireless networks with intrinsic secrecy. The aggregate interference has been characterized and the received SIR analyzed in both the legitimate and eavesdropping networks for different receiver selection strategies. Local

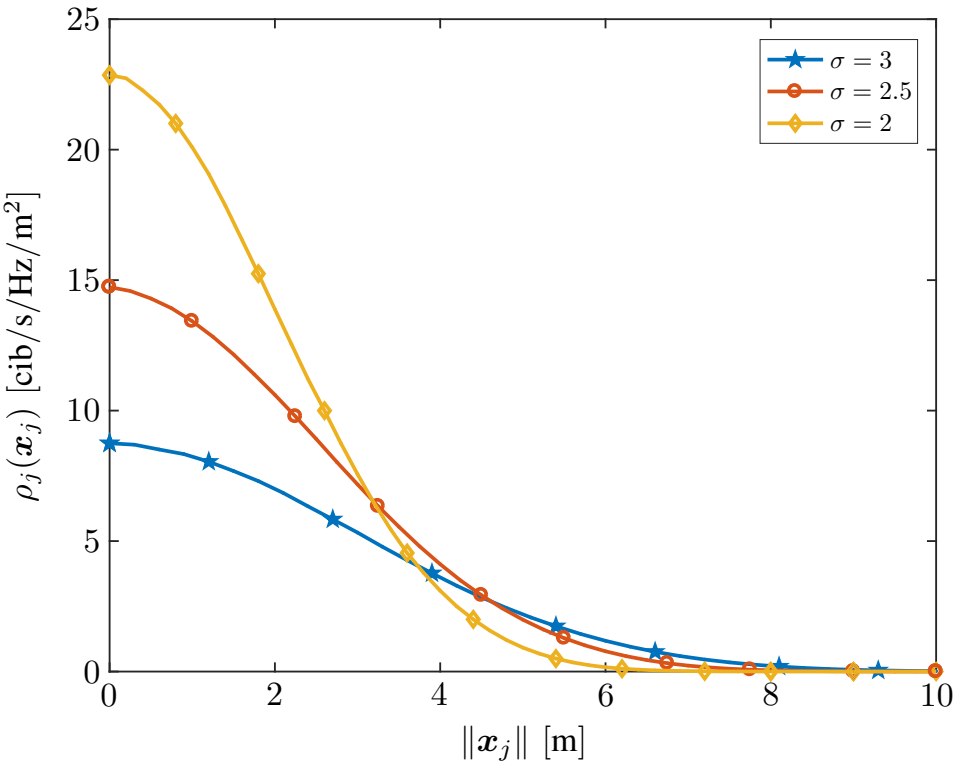

Figure 3.9: LNSRD in the SI-MS scenario comparing different variances σ^2 of the intensity functions $\lambda_{\text{tx}}(\boldsymbol{x})$, $\lambda_{\text{rx}}(\boldsymbol{x})$, and $\lambda_{\text{ex}}(\boldsymbol{x})$ while the IIN is not active. It has been considered $R_{\max} = 15$ [m], $|\mathcal{A}| \simeq 706$ [m^2], $\alpha_1 = 0.5$, $\alpha_2 = 0$, $\alpha_3 = 0.1$, $\lambda_{\text{h}} = 1$ [node/m^2], Rayleigh fading ($m = 1$), $b = 2$.

secrecy metrics have been defined to reveal the peculiar nature of the intrinsic secrecy for an inhomogeneous network from both the "link" and the "network" perspectives. Our findings show that interference engineering enables a desired secrecy rate (or throughput) density, despite of the low per-link secrecy rate. Global secrecy metrics have also been proposed to summarize the overall performance of different networks.

It has also been shown that a peak of density in the legitimate network guarantees a higher global confidentiality, despite the presence of a low-density region in which the local performance decays. Such an imbalance is particularly beneficial where the transmitters and the receivers of the legitimate network have overlapping density peaks. This suggest that the local secrecy level of an inhomogeneous network is mainly determined by the local density of legitimate nodes and that, from a network perspective, the

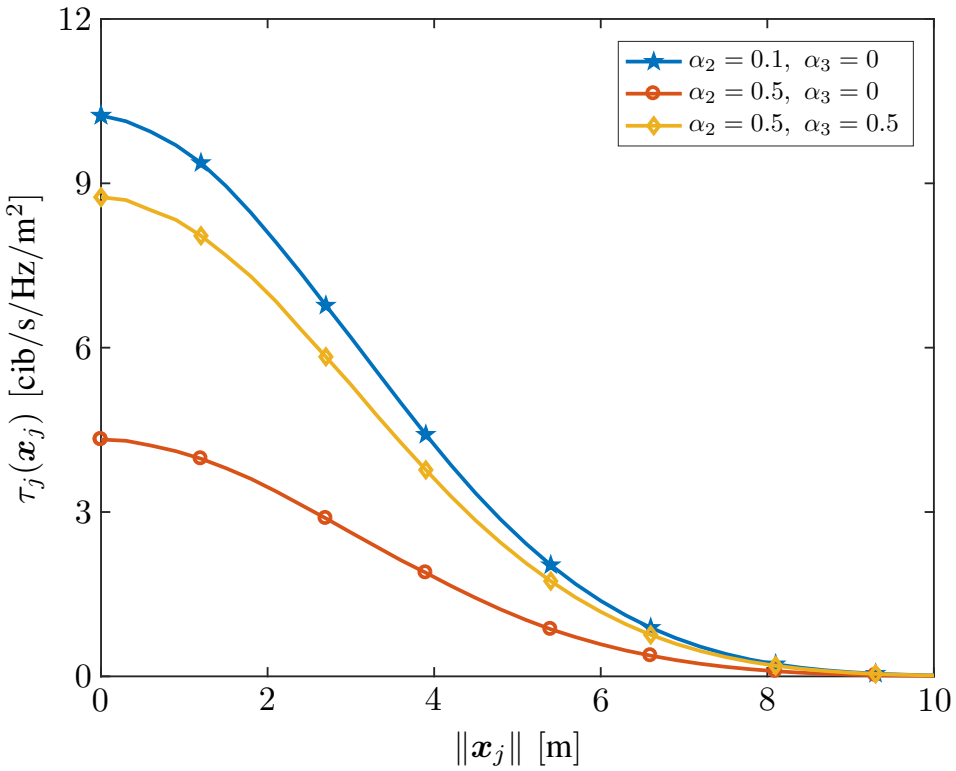

Figure 3.10: LNSTD in the SI-MS scenario comparing different network settings in terms of ratios α_2 and α_3. It has been considered $R_{\max} = 15$ [m], $\sigma = 3$ [m], $|\mathcal{A}| \simeq 706$ [m^2], $\alpha_1 = 0.5$, $\lambda_{\mathrm{h}} = 1$ [node/m^2], $R_{\mathrm{s}} = 4$ [cib/s/Hz], $P^{\star}_{\mathrm{so}} = 0.1$, Rayleigh fading ($m = 1$), $b = 2$.

performance loss in the low-density region is negligible with respect to the performance gain obtained in the high-density region.

We also found that to study an inhomogeneous network by modeling it as a superposition of homogeneous PPPs leads to a suboptimal performance analysis. In addition, the availability of legitimate receiver in dense regions is a key enabler for confidential communications.

The developed framework is particularly suitable for wireless networks applications that present an intrinsic inhomogeneity, such as heterogeneous access networks, cyber-physical systems, Internet of Things, and vehicular networks.

Chapter 4

Conclusion

This Ph.D. dissertation tackles the analysis and design of MWNs, to provide them with a reliable, resilient, and secure operation. The developed frameworks account for important spatial and temporal features of MWNs thus unleashing the full potential of the IoT and placing the first-mile toward the realization of the smart world era.

Specifically, Chapter 2 develops a spatiotemporal modeling for uncoordinated MWNs to account for their massive spatial existence and sporadic per-node traffic. The percentile-performance of the MWN are inspected w.r.t. the spatial traffic intensity, target transmission rate, and uncoordinated access protocol. Furthermore we assess the scalability limit of uncoordinated access, which is used in wireless networks either to transmit data or request scheduling, thus solving the bottlenecks of the access network. Our results show that to design a network by considering spatially averaged metrics only corresponds to a total uncertainty on the actual fraction of the network holding stability a target operation (e.g., stability). Furthermore, we show that dominant systems, which are commonly used to simplify the spatiotemporal analysis of wireless networks, do not provide tight performance bound. Differently our framework provides the fraction of the network holding a target performance. Moreover we show that variations of the F-ALOHA protocol with different power-ramping schemes can improve the γ-stability and γ-operativity. The importance of power-ramping design, which is a tecnique in which nodes do not have to account for any information besides the success or insuccess of their previous transmission, is manifested through a case study that shows that ramping-down the power after a properly designed number of retrials can improve the network percentile performance (20% more stable users compared to F-ALOHA only).

Chapter 3 deals with the delivery of confidential information in inhomoge-

neous MWNs with intrinsic secrecy. We analyze the effect of inhomogeneities of the node distribution by exploiting a fine-grain spatial model, thus exploring the fundamental limits of network intrinsic secrecy. We also compare local and global secrecy metrics to compare the intrinsic secrecy of networks with different types of inhomogeneity. The lesson learned is that local maxima of legitimate node density improve the global network secrecy. It is the combination of massive presence of legitimate transmitters and receivers that enables higher level of confidentiality. Thus, we make a step forward towards the use of information-theoretic secrecy in future generation wireless networks, to help cryptography-based systems in preserving the confidentiality information.

We hereafter present some future research directions:

- **Spatiotemporal modeling of cellular ntworks:** After considering uncoordinated access is important to consider uplink and downlink in cellular networks, to analyze the distribution of user delay also accounting for the cell load and verious user scheduling policies.

- **Spatiotemporal modeling of WIPT networks:** wireless transfer of information and power (WIPT) via radiofrequency radiation has long been regarded as a possibility for energizing low-power devices. Now that the advances in electroncs have made it feasible it is an interesting solution to supply smart devices. Our interest is in modeling the network as composed by information-energy queues, and to inspect the delay distribution in the presence of energetic constraints of the transmission.

- **Secrecy routing for multihop networks:** The help that intrinsic secrecy can provide to cryptographic systems have not been quantified yet. In the area of best-effort solutions to conceal confidential information, secrecy routing in multihop networks is a viable solution that tradeoffs secrecy and delay.

- **Spatiotemporal modeling of networks with intrinsic secrecy:** Network intrinsic secrecy allows legitimate users to exploit the secrecy capacity of the wireless channel thus concealing a certain amount of bits per time unit. We believe that a spatiotemporal analysis will help quantifying the extent to which information-theoretic secrecy can provide in helping cryptographyc systems.

Appendix A

A.1 Proof of Theorem 1

In (2.1a) we present the average success probability at every receiver as a variable depending on the receiver' location. By the ergodicity of the PPP, the distribution of the success probability along all the links in an infinite network is associated to the distribution of the success probability at the typical point, i.e., the origin, that accounts for all the possible realization of the point process. By this interpretation we define the conditional success probability at the typical point as a random variable by

$$\mathsf{p}_{n_{\mathrm{p}}} = \mathbb{P}\Big\{\frac{P_{n_{\mathrm{p}}}\mathsf{h}_{\circ}R^{-2\eta}}{(\mathsf{i}_{\circ}+\sigma^2)} > \theta|\Pi\Big\} \tag{A.1a}$$

$$= e^{-\theta_{n_{\mathrm{p}}}\sigma^2}\prod_{j\,:\,\mathbf{y}_j\in\Pi\setminus\mathbf{y}_{\circ}}\Big(\sum_{i=1}^{N_{\mathrm{p}}}\frac{\breve{p}_{\mathrm{a}}w^{[i]}}{1+\theta_{n_{\mathrm{p}},i}\|\mathbf{y}_j\|^{-2\eta}}+1-\breve{p}_{\mathrm{a}}\sum_{i=1}^{N_{\mathrm{p}}}w^{[i]}\Big) \tag{A.1b}$$

where (A.1b) follows from the exponential distribution of the channel, considering $\mathsf{i}_{\circ}=\sum_{j\,:\,\mathbf{y}_j\in\Pi\setminus\mathbf{y}_{\circ}}\mathsf{p}_j\mathsf{a}_j\mathsf{h}_j\|\boldsymbol{y}_j\|^{-2\eta}$,[1] $\theta_{n_{\mathrm{p}}}=\theta R^{2\eta}/P_{n_{\mathrm{p}}}$, $\theta_{n_{\mathrm{p}},i}=\theta_{n_{\mathrm{p}}}P_i$, and averaging over ALOHA with random channel selection, power distribution (by using Approximation 1), and channels (by using the LT of the channel).

[1]The receiver of the typical link is considered at the origin without any loss of generality.

Then, the b^{th} order moment is computed by definition as

$$M_{b,n_{\mathrm{p}}} = \mathbb{E}^{!\circ}\Big\{ e^{-b\theta_{n_{\mathrm{p}}}\sigma^2} \prod_{j\,:\,\mathbf{y}_j\in\mathsf{\Pi}\setminus\mathbf{y}_\circ} \Big(\sum_{i=1}^{N_{\mathrm{p}}} \frac{\breve{p}_{\mathrm{a}} w^{[i]}}{1+\theta_{n_{\mathrm{p}},i}\|\mathbf{y}_j\|^{-2\eta}} + 1 - \breve{p}_{\mathrm{a}} \sum_{i=1}^{N_{\mathrm{p}}} w^{[i]} \Big)^b \Big\} \tag{A.2a}$$

$$= e^{-b\theta_{n_{\mathrm{p}}}\sigma^2} \exp\Big\{ -\lambda \frac{\pi}{\eta} \sum_{k=1}^{b} \binom{b}{k} (-1)^{k+1} \cdot \int_0^\infty \Big(-\sum_{i=1}^{N_{\mathrm{p}}} \breve{p}_{\mathrm{a}} \frac{w^{[i]}\theta_{n_{\mathrm{p}},i}}{u+\theta_{n_{\mathrm{p}},i}} \Big)^k u^{\frac{1-\eta}{\eta}} du \Big\} \tag{A.2b}$$

where (A.2b) follows by applying the PGFL of the PPP, considering $(1+v)^b = \sum_{k=0}^{b} \binom{b}{k} v^k$, rearranging the terms, transforming to polar coordinates, and changing integration variable $u \triangleq \|\boldsymbol{y}_j\|^{2\eta}$, thus concluding the proof.

Appendix B

B.1 Proof of Theorem 2

Let $\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}$ be the number of LRs selectable by $\boldsymbol{x}_j$. If $n_{\mathcal{A}_{\mathcal{R}_j}} = 0$ the conditional CDF of $\mathsf{z}_{j,\check{k}}$ given $\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}} = 0$ is assumed to be $F_{\mathsf{z}_{j,\check{k}}|\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}=0}(z) = 1$. Conversely, if $n_{\mathcal{A}_{\mathcal{R}_j}} > 0$ it can be obtained as

$$\begin{aligned} F_{\mathsf{z}_{j,\check{k}}|\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}}(z) &= \mathbb{P}\left\{\mathsf{z}_{j,\check{k}} \leq z | \mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}} = n_{\mathcal{A}_{\mathcal{R}_j}}\right\} \\ &= \mathbb{P}\left\{\mathsf{z}_{j,1} \leq z, \mathsf{z}_{j,2} \leq z, \ldots, \mathsf{z}_{j,n_{\mathcal{A}_{\mathcal{R}_j}}} \leq z\right\} \\ &= \prod_{k=1}^{n_{\mathcal{A}_{\mathcal{R}_j}}} F_{\mathsf{z}_{j,k}}(z) = \left[F_{\mathsf{z}_{j,k}}(z)\right]^{n_{\mathcal{A}_{\mathcal{R}_j}}} \end{aligned} \tag{B.1}$$

where $\mathsf{z}_{j,k}$ have been assumed independent and identically distributed. The identical distribution is shown in (3.14b) and (3.16) for the generic receiver, while the assumption of independence of SIRs at different locations is assumed for tractability and verified [76]. Moreover, correlation is higher when the amount of common randomness is high, thus, massively dense networks, networks with random access, multiple channels, and multiple codes, suffer from low interference correlation [113,140]. By assuming that $\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}$ is a Poisson RV with intensity measure $\Lambda_{\mathrm{rx}}(\mathcal{A}_{\mathcal{R}_j})$, the CDF of $\mathsf{z}_{j,\check{k}}$ is obtained by the marginalization

$$\begin{aligned} F_{\mathsf{z}_{j,\check{k}}}(z) &= \mathbb{E}_{\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}}\left\{F_{\mathsf{z}_{j,\check{k}}|\mathsf{n}_{\mathcal{A}_{\mathcal{R}_j}}}(z)\right\} \\ &= e^{-\Lambda_{\mathrm{rx}}(\mathcal{A}_{\mathcal{R}_j})} + \sum_{n=1}^{\infty} e^{-\Lambda_{\mathrm{rx}}(\mathcal{A}_{\mathcal{R}_j})} \frac{(\Lambda_{\mathrm{rx}}(\mathcal{A}_{\mathcal{R}_j}))^n}{n!} \left[F_{\mathsf{z}_{j,k}}(z)\right]^n . \end{aligned} \tag{B.2}$$

The proof is then obtained by rearranging terms, also using the definition of the exponential function.

B.2 Proof of Corollary 2

The proof follows considering that (3.18), holding in the FIN setting, also holds for the FHN where $\Lambda_{\mathrm{rx}}(\mathcal{A}_{\mathcal{R}_j}) = |\mathcal{A}_{\mathcal{R}_j}|\lambda_{\mathrm{rx}} = \pi r_{\mathrm{M}}^2 \lambda_{\mathrm{rx}}$. Furthermore, since receiver locations are described by an HPPP on $\mathcal{A}_{\mathcal{R}_j}$, the squared distance $\mathsf{r}_{j,k}^2$ between $\boldsymbol{x}_j$ and a generic receiver x_k is a uniform RV $\mathcal{U}(0, r_{\mathrm{M}}^2]$. To conclude, it is sufficient to recall that the distribution of the aggregate interference of an homogeneous panorama of interferers in $\mathbb{R}^2$ (c.f. [93]) is the same in each point of the network (see (3.10b)-(3.11)).

B.3 Proof of Corollary 3

Since Corollary 3 is a special case of Theorem 2, (3.18) directly applies to compute the CDF of $\mathsf{z}_{j,\check{k}}$. Then, when the receivers are characterized by a HPPP, $\mathsf{r}_{j,k}$ and $\theta_{j,k}$ are independent, so that (3.14b) assumes the form of (3.19). Furthermore, for the homogeneity of receivers $\mathsf{r}_{j,k}^2 \sim \mathcal{U}(0, r_{\mathrm{M}}^2]$ and $\theta_{j,k} \sim \mathcal{U}(0, 2\pi]$.

B.4 Statistical characterization of the polar coordinates of the k^{th} closest receiver

Hereinafter, the distributions of RVs needed to perform expectations of (3.23) are characterized.

1. The PDF of the distance between the LT $\boldsymbol{x}_j$ and the k^{th} closest receiver is given by

$$f_{\mathsf{r}_{j,(k)}}(r) = \frac{d}{dr} F_{\mathsf{r}_{j,(k)}}(r) = \frac{d}{dr} \left(\mathbb{P}\left\{ \mathsf{r}_{j,(k)} \leq r \right\} \right) \tag{B.3}$$

where

$$\begin{aligned} \mathbb{P}\left\{ \mathsf{r}_{j,(k)} \leq r \right\} &= 1 - \mathbb{P}\left\{ \mathsf{r}_{j,(k)} > r \right\} \\ &= 1 - \mathbb{P}\left\{ \mathsf{n}_{\mathrm{rx}}(\mathcal{B}_j(r)) \leq k-1 \right\} \end{aligned} \tag{B.4}$$

and $\mathsf{n}_{\mathrm{rx}}(\mathcal{B}_j(r))$ is a Poisson RV with intensity measure $\Lambda_{\mathrm{rx}}(\mathcal{B}_j(r))$ representing the number of LRs in a ball with radius r and center $\boldsymbol{x}_j$, i.e., $\mathsf{n}_{\mathrm{rx}}(\mathcal{B}_j(r)) \sim \mathcal{P}\left(\Lambda_{\mathrm{rx}}(\mathcal{B}_j(r))\right)$.[1]

[1] $\mathcal{P}(\Lambda)$ denotes the distribution of a Poisson RV with parameter Λ.

2. The conditional PDF of the angle between the LT $\boldsymbol{x}_j$ and the k^{th} closest receiver given $\mathsf{r}_{j,(k)}$ is defined by

$$f_{\mathsf{\theta}_{j,(k)}|\mathsf{r}_{j,(k)}}(\theta) = \frac{\lambda_{\text{rx}}(r_{j,(k)}, \theta)}{\Lambda_{\text{rx}}(\mathcal{C}_{j,(k)})} \tag{B.5}$$

where $\mathcal{C}_{j,(k)}$ is a circumference centered at $\boldsymbol{x}_j$ with radius $r_{j,(k)}$ and $\Lambda_{\text{rx}}(\mathcal{C}_{j,(k)})$ is the mean number of LRs on $\mathcal{C}_{j,(k)}$.

Bibliography

[1] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khereishan, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data managment, security and enabling technologies," *IEEE Commun. Surveys Tuts.*, to be published 2017.

[2] M. Roopaei, P. Rad, and K. K. R. Choo, "Cloud of things in smart agriculture: Intelligent irrigation monitoring by thermal imaging," *IEEE Cloud Computing*, vol. 4, no. 1, pp. 10–15, Jan. 2017.

[3] S. Roy, R. Ray, A. Roy, S. Sinha, G. Mukherjee, S. Pyne, S. Mitra, S. Basu, and S. Hazra, "Iot, big data science analytics, cloud computing and mobile app based hybrid system for smart agriculture," in *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, Aug. 2017, pp. 303–304.

[4] S. R. Prathibha, A. Hongal, and M. P. Jyothi, "Iot based monitoring system in smart agriculture," in *2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT)*, Mar. 2017, pp. 81–84.

[5] B. R. Haverkort and A. Zimmermann, "Visual networking index," *IEEE Internet Computing*, vol. 21, no. 1, pp. 8–10, 2017.

[6] M. W. Condry and C. B. Nelson, "Using smart edge IoT devices for safer, rapid response with industry IoT control operations," *Proc. IEEE*, vol. 104, no. 5, pp. 938–946, May 2016.

[7] Q. Fei, "Distributed dynamic network, cellular based solution for smart industry," in *2015 Asia-Pacific Microwave Conference (APMC)*, vol. 1, Dec. 2015, pp. 1–1.

[8] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid – the new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, Fourthquarter 2012.

[9] D. He, S. Chan, and M. Guizani, "Win-win security approaches for smart grid communications networks," *IEEE Netw.*, vol. 31, no. 6, pp. 122–128, Nov. 2017.

[10] R. Morello, S. C. Mukhopadhyay, Z. Liu, D. Slomovitz, and S. R. Samantaray, "Advances on sensing technologies for smart cities and power grids: A review," *IEEE Sensors J.*, vol. 17, no. 23, pp. 7596–7610, Dec. 2017.

[11] S. N. A. U. Nambi, R. V. Prasad, and A. R. Lua, "Decentralized energy demand regulation in smart homes," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 3, pp. 372–380, Sep. 2017.

[12] Y. T. Lee, W. H. Hsiao, Y. S. Lin, and S. C. T. Chou, "Privacy-preserving data analytics in cloud-based smart home with community hierarchy," *IEEE Trans. Consum. Electron.*, vol. 63, no. 2, pp. 200–207, May 2017.

[13] ——, "Privacy-preserving data analytics in cloud-based smart home with community hierarchy," *IEEE Transactions on Consumer Electronics*, vol. 63, no. 2, pp. 200–207, May 2017.

[14] I. Hwang and Y. J. Jang, "Process mining to discover shoppers – pathways at a fashion retail store using a wifi-base indoor positioning system," *IEEE Trans. Autom. Sci. Eng.*, vol. 14, no. 4, pp. 1786–1792, Oct. 2017.

[15] K. Nur, M. Morenza-Cinos, A. Carreras, and R. Pous, "Projection of rfid-obtained product information on a retail stores indoor panoramas," *IEEE Intell. Syst.*, vol. 30, no. 6, pp. 30–37, Nov. 2015.

[16] B. F. Wu, W. J. Tseng, Y. S. Chen, S. J. Yao, and P. J. Chang, "An intelligent self-checkout system for smart retail," in *2016 International Conference on System Science and Engineering (ICSSE)*, Jul. 2016, pp. 1–4.

[17] Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu, "Vehicular social networks: Enabling smart mobility," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 16–55, May 2017.

[18] Y. Liu, X. Weng, J. Wan, X. Yue, H. Song, and A. V. Vasilakos, "Exploring data validity in transportation systems for smart cities," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 26–33, May 2017.

[19] Z. Ding, B. Yang, Y. Chi, and L. Guo, "Enabling smart transportation systems: A parallel spatio-temporal database approach," *IEEE Trans. Comput.*, vol. 65, no. 5, pp. 1377–1391, May 2016.

[20] S. J. Olshansky, B. A. Carnes, Y. C. Yang, N. Miller, J. Anderson, H. Beltrn-Snchez, and K. Ricanek, "The future of smart health," *IEEE Computer*, vol. 49, no. 11, pp. 14–21, Nov. 2016.

[21] G. Muhammad, S. M. M. Rahman, A. Alelaiwi, and A. Alamri, "Smart health solution integrating iot and cloud: A case study of voice pathology monitoring," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 69–73, Jan. 2017.

[22] H. Thapliyal, V. Khalus, and C. Labrado, "Stress detection and management: A survey of wearable smart health devices," *IEEE Trans. Consum. Electron.*, vol. 6, no. 4, pp. 64–69, Oct. 2017.

[23] C. E. Jimnez, A. Solanas, and F. Falcone, "Stress detection and management: A survey of wearable smart health devices," *IEEE Computer*, vol. 47, no. 10, pp. 22–24, 2014.

[24] J. V. Lucke, "Smart government – the potential of intelligent networking in government and public administration," in *2016 Conference for E-Democracy and Open Government (CeDEM)*, May 2016, pp. 137–144.

[25] J. Aguilar, "Tutorial: Data analytics in the domain of smart cities and e-government," in *2016 Third International Conference on eDemocracy eGovernment (ICEDEG)*, Mar. 2016, pp. 1–4.

[26] N. Chen and Y. Yamashita, "The possibility for the active use of smart devices in university education," in *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, July 2017, pp. 99–104.

[27] S. Babi, M. Krei, and K. Kucel, "E-education 2.0: Students' digital identity and online learning activities," in *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, May 2014, pp. 756–761.

[28] S. Pellicer, G. Santa, A. Bleda, R. Maestre, A. Jara, and A. G. Skarmeta, "A global perspectife of smart cities: A survey," in *Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Oct. 2013, pp. 439–444.

[29] V. Fernandez-Anez, "Stakeholders approach to smart cities: A survey on smart city definitions," in *in Proceedings of the First International Conference, Smart-CT 2016, Mlaga, Spain.* Springer Cham, 2016, pp. 157–167.

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

[31] C. Perera, A. Zaslavsky, M. Compton, P. Christen, and D. Georgakopoulos, "Semantic-driven configuration of the internet of things middleware," in *IEEE 9th International Conference on Semantics, Knowledge and Grids*, 2013, pp. 66–73.

[32] X. Cao, L. Liu, Y. Cheng, and X. Shen, "Towards energy-efficient wireless networking in the big data era: A survey," *IEEE Commun. Surveys Tuts.*, vol. PP, no. 99, pp. 1–1, 2017.

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

[34] S. Landset, T. M. Khoshgoftaar, A. N. Richter, and T. Hasanin, "A survey of open source tools for machine learning with big data in the Hadoop ecosystem," *Journal of Big Data*, vol. 2, no. 1, 2015.

[35] C. Zhu, H. Zhou, V. C. M. Leung, K. Wang, Y. Zhang, and L. T. Yang, "Toward big data in green city," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 14–18, Nov. 2017.

[36] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context aware computing, learning and big data in internet of things: A survey," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–30, 2017.

[37] C. Zhu, H. Zhou, V. C. M. Leung, K. Wang, and Y. Zhang, "Towards big data in green city," *IEEE Trans. Comput.*, vol. 55, no. 11, pp. 14–18, Nov. 2017.

[38] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. D. Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, Jun. 2017.

[39] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, Thirdquarter 2016.

[40] "Annual Global Road Crash Statistics," Association of Safe International Road Travel. [Online]. Available: https://asirt.org/Initiatives/Informing-Road-Users/Road-Safety-Facts/Road-Crash-Statistics

[41] "Road Safety: Basic Facts," World Health Organization, 2015. [Online]. Available: http://www.who.int/violence_injury_prevention/publications/road_traffic/Media_brief_all_factsheets_web.pdf?ua=1

[42] "National Highway Traffic Safety Association," National Highway Traffic Safety Administration. [Online]. Available: http://www.nhtsa.gov/Data/Traffic-Records

[43] "The Cost of Traffic Jams," The Economist, 2014. [Online]. Available: http://www.economist.com/blogs/economist-explains/2014/11/economist-explains-1

[44] D. Dardari, A. Conti, U. J. Ferner, A. Giorgetti, and M. Z. Win, "Ranging with ultrawide bandwidth signals in multipath environments," *Proc. IEEE*, vol. 97, no. 2, pp. 404–426, Feb. 2009, special issue on *Ultra-Wide Bandwidth (UWB) Technology & Emerging Applications*.

[45] M. Z. Win, A. Conti, S. Mazuelas, Y. Shen, W. M. Gifford, D. Dardari, and M. Chiani, "Network localization and navigation via cooperation," *IEEE Commun. Mag.*, vol. 49, no. 5, pp. 56–62, May 2011.

[46] A. Conti, M. Guerra, D. Dardari, N. Decarli, and M. Z. Win, "Network experimentation for cooperative localization," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 467–475, Feb. 2012.

[47] A. Conti, D. Dardari, M. Guerra, L. Mucchi, and M. Z. Win, "Experimental characterization of diversity navigation," *IEEE Syst. J.*, vol. 8, no. 1, pp. 115–124, Mar. 2014.

[48] S. Bartoletti, W. Dai, A. Conti, and M. Z. Win, "A mathematical model for wideband ranging," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 2, pp. 216–228, Mar. 2015.

[49] L. H. Sun, "Most americans will get a wrong or late diagnosis at least once in their lives," Washington Post, 2015.

[50] D. S. Nunes, P. Zhang, and J. S. Silva, "A survey on human-in-the-loop applications towards an Internet of all," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 944–965, Secondquarter 2015.

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

[52] Cisco, "Visual networking index," *White paper, Available: www.Cisco.com*, Feb. 2015.

[53] "High efficiency video coding," *document Rec. H.265, ITU-T SG13*, Apr. 2013.

[54] T. S. Rappaport, W. Roh, and K. Cheun, "Wireless engineers long considered high frequencies worthless for cellular systems. they couldn't be more wrong," *IEEE Spectr.*, vol. 51, no. 9, pp. 34–58, Sep. 2014.

[55] T. S. Rappaport, G. R. Maccartney, M. K. Samimi, and S. Sun, "Wideband millimeter-wave propagation measurements and channel models for future wireless communication system design," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 33 029–3056, Sep. 2015.

[56] I. Yaqoob, I. A. T. Hashem, Y. Mehmood, A. Gani, S. Mokhtar, and S. Guizani, "Enabling communication technologies for smart cities," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 112–120, Jan. 2017.

[57] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[58] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[59] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *Ad Hoc Networks*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[60] A. Biral, MarcoCentenaro, A. Zanella, L. Vangelista, and M. Zorzi, "The challenges of M2M massive access in wireless cellular networks," *Digital Communications and Networks*, vol. 1, no. 1, pp. 1–19, Feb. 2015.

[61] A. Bader, H. ElSawy, M. Gharbieh, M. S. Alouini, A. Adinoyi, and F. Alshaalan, "First mile challenges for large-scale IoT," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 138–144, March 2017.

[62] 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.

[63] M. S. Ali, E. Hossain, and D. I. Kim, "LTE/LTE-A random access for massive machine-type communications in smart cities," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 76–83, January 2017.

[64] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios," *IEEE Wireless Commun. Mag.*, vol. 23, no. 5, pp. 60–67, Oct. 2016.

[65] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, Secondquarter 2017.

[66] D. Eckhoff and I. Wagner, "Privacy in the smart city – applications, technologies, challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. PP, no. 99, pp. 1–1, 2017.

[67] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, Thirdquarter 2015.

[68] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. PP, no. 99, pp. 1–1, 2017.

[69] A. Stahlbrost, A. Padyab, A. Stallstrom, and D. Hollosi, "Design of smart city systems from a privacy perspective," *International Journal on WWW/Internet*, vol. 13, no. 1, 2015.

[70] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[71] L. Mucchi, L. S. Ronga, and L. Cipriani, "A new modulation for intrinsically secure radio channel in wireless systems," *Springer Wireless Personal Communications*, vol. 51, no. 1, pp. 67–80, Sep. 2008.

[72] P. A. Regalia, A. Khisti, Y. Liang, and S. Thomasin, "Secure communications via physical-layer and information-theoretic techniques," *Proc. IEEE*, vol. 103, no. 10, pp. 1698–1701, Oct. 2015.

[73] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[74] M. Z. Win, A. Rabbachin, J. Lee, and A. Conti, "Cognitive network secrecy with interference engineering," *IEEE Netw.*, vol. 28, no. 5, pp. 86 – 90, Sep./Oct. 2014.

[75] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

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

[77] P. C. Pinto, J. O. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks – Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[78] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764 –2775, Aug. 2011.

[79] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: a stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, Jun. 2013.

[80] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[81] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*. Springer, 2016.

[82] H.-M. Wang, C. Wang, T.-X. Zheng, and T. Q. S. Quek, "Impact of artificial noise on cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7390–7404, Nov. 2016.

[83] 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. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.

[84] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Commun.*, vol. 15, no. 8, pp. 5651–5663, Aug. 2016.

[85] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 278–292, Jan. 2017.

[86] M. Z. Win, L. Ruan, A. Rabbachin, Y. Shen, and A. Conti, "Multi-tier network secrecy in the ether," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 28–32, Jun. 2015.

[87] O. Andrisano, A. Conti, D. Dardari, B. M. Masini, and G. Pasolini, "Bluetooth and IEEE802.11 coexistence: Analytical performance evaluation in fading channel," in *IEEE Personal, Indoor, and Mobile Radio Communications Conference, PIMRC 2002*, Lisbon, Sep. 2002.

[88] M. Chiani, A. Conti, and C. Fontana, "Improved performance in TD-CDMA mobile radio system by optimizing energy partition in channel estimation," *IEEE Trans. Commun.*, vol. 51, no. 3, pp. 352–355, Mar. 2003.

[89] A. Conti, B. M. Masini, F. Zabini, and O. Andrisano, "On the downlink performance of multi-carrier CDMA systems with partial equalization," *IEEE Trans. Wireless Commun.*, vol. 6, no. 1, pp. 230–239, Jan. 2007.

[90] A. Conti, D. Panchenko, S. Sidenko, and V. Tralli, "Log-concavity property of the error probability with application to local bounds for wireless communications," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2766–2775, Jun. 2009.

[91] A. Conti, W. M. Gifford, M. Z. Win, and M. Chiani, "Optimized simple bounds for diversity systems," *IEEE Trans. Commun.*, vol. 57, no. 9, pp. 2674–2685, Sep. 2009.

[92] W. M. Gifford, A. Conti, M. Chiani, and M. Z. Win, "On the SNR penalties of ideal and non-ideal subset diversity systems," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3708–3724, Jun. 2012.

[93] M. Z. Win, P. C. Pinto, and L. A. Shepp, "A mathematical theory of network interference and its applications," *Proc. IEEE*, vol. 97, no. 2, pp. 205–230, Feb. 2009, special issue on *Ultra-Wide Bandwidth (UWB) Technology & Emerging Applications*.

[94] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.

[95] 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, 2013.

[96] H. ElSawy, A. S. Salem, M.-S. Alouini, and M. Z. Win, "Modeling and analysis of cellular networks using stochastic geometry: A tutorial," *IEEE Commun. Surveys Tuts.*, 2017, to appear.

[97] J. F. Kingman, *Poisson Processes*. Oxford University Press, 1993.

[98] D. Daley and D. Vere-Jones, *An Introduction to the Theory of Point Processes, Volume I: Elementary Theory and Methods*. Springer, 2003.

[99] ——, *An Introduction to the Theory of Point Processes, Volume II: General Theory and Structure*. Springer, 2008.

[100] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge University Press, 2012.

[101] M. Z. Win, P. C. Pinto, A. Giorgetti, M. Chiani, and L. A. Shepp, "Error performance of ultrawideband systems in a Poisson field of narrowband interferers," in *Proc. IEEE Int. Symp. on Spread Spectrum Tech. & Applicat.*, Manaus, Brazil, Aug. 2006, pp. 410–416.

[102] M. Z. Win, "A mathematical model for network interference," IEEE Communication Theory Workshop, Sedona, AZ, May 2007.

[103] P. C. Pinto and M. Z. Win, "Communication in a Poisson field of interferers – Part I: Interference distribution and error probability," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2176–2186, Jul. 2010.

[104] ——, "Communication in a Poisson field of interferers – Part II: Channel capacity and interference spectrum," *IEEE Trans. Wireless Commun.*, vol. 9, no. 7, pp. 2187–2195, Jul. 2010.

[105] ——, "Spectral characterization of wireless networks," *IEEE Wireless Commun. Mag.*, vol. 14, no. 6, pp. 27–31, Dec. 2007, special Issue on *Wireless Sensor Networking*.

[106] A. Rabbachin, T. Q. Quek, P. C. Pinto, I. Oppermann, and M. Z. Win, "Non-coherent UWB communication in the presence of multiple narrowband interferers," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3365–3379, Nov. 2010.

[107] P. C. Pinto, A. Giorgetti, M. Z. Win, and M. Chiani, "A stochastic geometry approach to coexistence in heterogeneous wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1268–1282, Sep. 2009, special issue on *Stochastic Geometry and Random Graphs for Wireless Networks*.

[108] A. Rabbachin, T. Q. Quek, H. Shin, and M. Z. Win, "Cognitive network interference," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 480–493, Feb. 2011.

[109] L. Ruan, V. K. Lau, and M. Z. Win, "Generalized interference alignment – Part I: Theoretical framework," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2675–2687, May 2016.

[110] ——, "Generalized interference alignment – Part II: Application to wireless secrecy," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2688–2701, May 2016.

[111] J. Lee, A. Conti, A. Rabbachin, and M. Z. Win, "Distributed network secrecy," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1889–1900, Sep. 2013.

[112] P. C. Pinto, J. O. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks – Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.

[113] M. Haenggi, "The meta distribution of the SIR in Poisson bipolar and cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2577–2589, Apr. 2016.

[114] H. ElSawy and M. S. Alouini, "On the meta distribution of coverage probability in uplink cellular networks," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1625–1628, July 2017.

[115] D. S. Nunes, P. Zhang, and J. S. Silva, "A survey on human-in-the-loop applications towards an Internet of all," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 944–965, Secondquarter 2015.

[116] A. Laya, C. Kalalas, F. Vazquez-Gallego, L. Alonso, and J. Alonso-Zarate, "Goodbye, ALOHA!" *IEEE Access*, vol. 4, pp. 2029–2044, 2016.

[117] A. Bader, H. ElSawy, M. Gharbieh, M.-S. Alouini, A. Adinoyi, and F. Alshaalan, "First mile challenges for large-scale IoT," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 138–144, Mar. 2017.

[118] L. Vangelista, A. Zanella, and M. Zorzi, "Long-range IoT technologies: The dawn of LoRa?" in *Future Access Enablers of Ubiquitous and Intelligent Infrastructures*. Springer, 2015, pp. 51–58.

[119] R. R. Rao and A. Ephremides, "On the stability of interacting queues in a multiple–access system," *IEEE Trans. Inf. Theory*, vol. 34, no. 5, pp. 918–930, Sep. 1988.

[120] V. Anantharam, "The stability region of the finite-user slotted ALOHA protocol," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 535–540, May 1991.

[121] W. Luo and A. Ephremides, "Stability of N interacting queues in random–access systems," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1579–1587, Jul. 1999.

[122] A. Ephremides and R.-Z. Zhu, "Delay analysis of interacting queues with an approximate model," *IEEE Trans. Commun.*, vol. 35, no. 2, pp. 194–201, Feb 1987.

[123] L. Tassiulas and A. Ephremides, "Dynamic server allocation to parallel queues with randomly varying connectivity," *IEEE Trans. Inf. Theory*, vol. 39, no. 2, pp. 466–478, Mar 1993.

[124] M. J. Neely, "Order optimal delay for opportunistic scheduling in multi-user wireless uplinks and downlinks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 5, pp. 1188–1199, Oct 2008.

[125] N. Pappas, M. Kountouris, and A. Ephremides, "The stability region of the two-user interference channel," in *Proc. IEEE Inf. Theory Workshop*, no. 5, Sep. 2013, pp. 1–5.

[126] N. Pappas and M. Kountouris, "The stability region of the two-user broadcast channel," in *Proc. IEEE Int. Conf. Commun.*, no. 5, May 2016, pp. 1–6.

[127] G. D. Çelik and E. Modiano, "Scheduling in networks with time-varying channels and reconfiguration delay," *IEEE/ACM Trans. Netw.*, vol. 23, no. 1, pp. 99–113, Feb. 2015.

[128] M. J. Neely, E. Modiano, and C. E. Rohrs, "Dynamic power allocation and routing for time-varying wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 1, pp. 89–103, Jan 2005.

[129] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless network," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.

[130] H. ElSawy, A. S. Salem, M.-S. Alouini, and M. Z. Win, "Modeling and analysis of cellular networks using stochastic geometry: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 167–203, Firstquarter 2017.

[131] L. H. Afify, H. ElSawy, T. Y. Al-Naffouri, and M. S. Alouini, "A unified stochastic geometry model for mimo cellular networks with retransmissions," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8595–8609, Dec 2016.

[132] R. Arshad, H. ElSawy, S. Sorour, T. Y. Al-Naffouri, and M. S. Alouini, "Velocity-aware handover management in two-tier cellular networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1851–1867, March 2017.

[133] 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.

[134] K. S. Ali, H. ElSawy, M. Haenggi, and M. S. Alouini, "The effect of spatial interference correlation and jamming on secrecy in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 4, pp. 530–533, Aug 2017.

[135] 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.

[136] A. H. Sakr and E. Hossain, "Analysis of k-tier uplink cellular networks with ambient rf energy harvesting," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2226–2238, Oct 2015.

[137] K. Stamatiou and M. Haenggi, "Random-access poisson networks: Stability and delay," *IEEE Commun. Lett.*, vol. 14, no. 11, pp. 1035–1037, November 2010.

[138] P. H. J. Nardelli, M. Kountouris, P. Cardieri, and M. Latva-aho, "Throughput optimization in wireless networks under stability and packet loss constraints," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1883–1895, Aug 2014.

[139] Y. Zhong, M. Haenggi, T. Q. S. Quek, and W. Zhang, "On the stability of static Poisson networks under random access," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 2985–2998, Jul. 2016.

[140] M. Gharbieh, H. ElSawy, A. Bader, and M. Alouini, "Spatiotemporal stochastic modeling of IoT enabled cellular networks: Scalability and stability analysis," *IEEE Trans. Commun.*, no. 99, 2017.

[141] G. Chisci, H. ElSawy, A. Conti, M.-S. Alouini, and M. Z. Win, "On the scalability of uncoordinated multiple access for the Internet of Things," in *2017 International Symposium on Wireless Communication Systems (ISWCS)*, Aug. 2017, pp. 402–407.

[142] ——, "Spatiotemporal modeling of uncoordinated massive wireless networks," *IEEE/ACM Trans. Netw.*, To be submitted 2017.

[143] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge, UK: Cambridge University Press, 2013.

[144] V. Chandrasekhar and J. G. Andrews, "Spectrum allocation in tiered cellular networks," *IEEE Trans. Commun.*, vol. 57, no. 10, pp. 3059–3068, October 2009.

[145] L. Yang, S. H. Song, and K. B. Letaief, "Optimal overlay cognitive spectrum access with f-aloha in macro-femto heterogeneous networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1323–1335, Feb 2016.

[146] G. George, R. K. Mungara, A. Lozano, and M. Haenggi, "Ergodic spectral efficiency in MIMO cellular networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2835–2849, May 2017.

[147] A. S. Alfa, *Applied Discrete-Time Queues*, 2nd ed. Springer, 2016.

[148] Y. Zhou and W. Zhuang, "Performance analysis of cooperative communication in decentralized wireless networks with unsaturated traffic," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3518–3530, May 2016.

[149] L. Sartori and S. E. Elayoubi and B. Fourestie and Z. Nouir, "On the WiMAX and HSDPA coexistence," in *IEEE International Conference on Communications*, Jun. 2007, pp. 5636–5641.

[150] R. M. Loynes, "The stability of a queue with non-independent interarrival and service times," *Proc. Cambridge Philosphical Society*, vol. 58, no. 5, pp. 497–520, 1962.

[151] K. D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, May 2012.

[152] Y. Zhang, G. Li, Q. Du, G. Lyu, and G. Zhang, "High-rate cooperative beamforming for physical-layer security in wireless cyber-physical systems," in *Commun. Workshops, IEEE Int. Conf. Commun. (ICCW)*, Jun. 2015, pp. 2622–2626.

[153] K. Ly and Y. Jin, "Security challenges in CPS and IoT: From end-node to the system," *IEEE Computer Society Annu. Symp. VLSI (ISVLSI)*, pp. 63–68, Jul. 2016.

[154] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.

[155] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan. 2015.

[156] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, 2016.

[157] A. Bazzi, B. M. Masini, and A. Zanella, "Performance analysis of V2V beaconing using LTE in direct mode with full duplex radios," *IEEE Commun. Lett.*, vol. 4, no. 6, pp. 685–688, Dec. 2015.

[158] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, Fourthquarter 2015.

[159] J. C. Rolfe, *Svetonius, Lives of Caesars*, L. C. Library, Ed. Harvard University Press, 1998, vol. I.

[160] D. Kahn, *The Codebreakers, The Story of Secret Writing*, Macmillan, Ed., New York, NY, USA, 1967.

[161] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–652, Nov. 1976.

[162] M. Hellman, "An extension of the shannon theory approach to cryptography," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 3, pp. 289–294, May 1977.

[163] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in IoT: A novel perspective," *MDPI Information*, vol. 49, no. 7, pp. 1–17, Aug. 2016.

[164] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[165] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[166] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[167] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[168] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[169] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 29, no. 10, pp. 2067–2076, Dec. 2011.

[170] S. A. A. Fakoorian, H. Jafarkhani, and A. L. Swindlehurst, "Secure space-time block coding via artificial noise alignment," in *Proc. Asilomar Conf. on Signals, Systems, and Computers*, Monterey, CA, USA, Nov. 2011, pp. 651 – 655.

[171] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1568 – 1571, Aug. 2013.

[172] J. P. Vilela, M. Bloch, J. Barros, and S. W. Mclaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[173] L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *Proc. IEEE Global Telecomm. Conf.*, Miami, FL, USA, Dec. 2010, pp. 1–6.

[174] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[175] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[176] H. ElSawy and E. Hossain, "On stochastic geometry modeling of cellular uplink transmission with truncated channel inversion power control," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4454–4469, Aug. 2014.

[177] 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, Aug. 2013.

[178] J. G. Andrews, R. K. Ganti, M. Haenggi, N. Jindal, and S. Weber, "A primer on spatial modeling and analysis in wireless networks," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 156–163, Nov. 2010.

[179] N. Deng, W. Zhou, and M. Haenggi, "The Ginibre point process as a model for wireless networks with repulsion," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 107–121, Jan. 2015.

[180] R. K. Ganti and M. Haenggi, "Interference and outage in clustered wireless ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4067–4086, Sep. 2009.

[181] N. Deng, W. Zhou, and M. Haenggi, "Heterogeneous cellular network models with dependence," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2167–2181, Oct. 2015.

[182] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 2, no. 3, pp. 257–269, Sep. 2003.

[183] Z. Gong and M. Haenggi, "Interference and outage in mobile random networks: Expectation, distribution, and correlation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 337–349, Feb. 2014.

[184] N. Lu, T. H. Luan, M. Wang, X. Shen, and F. Bai, "Capacity and delay analysis for social-proximity urban vehicular networks," in *Proc. IEEE Conf. on Computer Commun. (INFOCOM)*, Mar. 2012, pp. 1476–1484.

[185] E. Steinmetz, M. Wildemeersch, T. Q. S. Quek, and H. Wymeersch, "A stochastic geometry model for vehicular communication near intersections," in *Proc. IEEE Global Telecomm. Conf. Workshops*, Dec. 2015, pp. 1–6.

[186] F. Zabini and A. Conti, "Inhomogeneous Poisson sampling of finite-energy signals with uncertainties in $\mathbb{R}^d$," *IEEE Trans. Signal Process.*, vol. 64, no. 18, pp. 4679–4694, Sep. 2016.

[187] G. Chisci, A. Conti, L. Mucchi, and M. Z. Win, "Maximum secrecy rate in inhomogeneous poisson networks," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2017, pp. 2102–2106.

[188] ——, "Intrinsic secrecy in inhomogeneous stochastic networks," *IEEE/ACM Trans. Netw.*, Accepted 2017.

[189] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, 3rd ed., ser. Wiley Series in Probability and Statistics. Wiley, 2013.

[190] J. Gil-Pelaez, "Note on the inversion theorem," *Biometrika*, vol. 38, no. 3/4, pp. 481–482, Dec. 1951.

[191] D. P. Bertsekas and J. N. Tsitsiklis, *Introduction to Probability*. Athena Scientific, 2008.

[192] H. R. Thompson, "Distribution of distance to n-th neighbour in a population of randomly distributed individuals," *Ecology*, vol. 37, no. 2, pp. 391–394, Apr. 1956.

[193] S. Srinivasa and M. Haenggi, "Distance distribution in finite uniformly random networks: Theory and applications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 940–949, Feb. 2010.

[194] D. P. Bertsekas and R. G. Gallager, *Data Networks*, 2nd ed. New Jersey, 07632: Prentice-Hall, 1992.

Author's Publications

[1] G. Chisci, H. ElSawy, A. Conti, M.-S. Alouini, and M. Z. Win, "Spatiotemporal modeling for uncoordinated massive wireless networks," *IEEE/ACM Trans. Netw.*, under review 2017.

[2] G. Chisci, A. Conti, L. Mucchi, and M. Z. Win, "Intrinsic secrecy in inhomogeneous stochastic networks," *IEEE/ACM Trans. Netw.*, accepted with minor revision 2017.

[3] L. Mucchi, L. S. Ronga, and G. Chisci, "Noise-loop multiple access," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8255–8266, Oct. 2016.

[4] G. Chisci, H. ElSawy, A. Conti, M.-S. Alouini, and M. Z. Win, "On the scalability of uncoordinated multiple access for the Internet of Things," in *2017 International Symposium on Wireless Communication Systems (ISWCS)*, Aug. 2017, pp. 402–407, **winner of the "Best scientific contribution to the conference" award**.

[5] G. Chisci, A. Conti, L. Mucchi, and M. Z. Win, "Maximum secrecy rate in inhomogeneous poisson networks," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2017, pp. 2102–2106.

[6] L. Mucchi, G. Chisci, E. D. Re, and L. S. Ronga, "Noise-loop multiple access for wireless communications," in *2015 IEEE International Conference on Communication Workshop (ICCW)*, Jun. 2015, pp. 2097–2101.