Using Outage Probability to Tailor Communication Protocols Suitable for Cyber-Physical Systems Operating in Confined Areas

Van Lan Dao
USING OUTAGE PROBABILITY TO TAILOR COMMUNICATION PROTOCOLS SUITABLE FOR CYBER-PHYSICAL SYSTEMS OPERATING IN CONFINED AREAS

Van-Lan Dao

2023

School of Innovation, Design and Engineering
USING OUTAGE PROBABILITY TO TAILOR COMMUNICATION PROTOCOLS
SUITABLE FOR CYBER-PHYSICAL SYSTEMS OPERATING IN CONFINED AREAS

Van-Lan Dao

Akademisk avhandling

som för avläggande av teknologie doktorsexamen i datavetenskap vid
Akademin för innovation, design och teknik kommer att offentligen försvaras
fredagen den 13 oktober 2023, 13.30 i Paros, Mälardalens universitet, Västerås.

Fakultetsopponent: Professor Viktoria Fodor, KTH Royal Institute of Technology
Abstract

Some types of Cyber-Physical System (CPS) applications found within e.g., quarrying, mining, harbors, and construction sites, operate within confined areas. To guarantee that communications between nodes in such systems operate smoothly, the adopted wireless communication protocols must meet stringent requirements, even in the presence of interference and/or jamming. This thesis work targets finding performance metrics suitable for designing and evaluating wireless networks when used for CPSs in confined areas. Given the shortage of spectrum and the increased risk of cyber-attacks experienced lately, the protocols must also be adjusted to perform well when subject to strong interference and/or adversary jamming. Hence, to be useful in practice, metrics that can be recalculated during runtime are needed, such that they can be used not only to propose, select and tailor the communication protocols to fulfill the stringent CPS requirements but also to optimize their performance during runtime. The literature survey conducted in this thesis shows that a reliability metric in terms of thresholding the so-called outage probability is valuable for all design steps as well as for continuously optimizing the communications. However, since the outage probability is defined as the probability that an individual wireless link will experience outage, it does not address the reliability of the entire network within the confined area. The thesis work shows that it is possible to consider overall outage probabilities and evaluates the probability of outage for each individual packet from a specific source node to a final destination, including all possible links in the network. This way, it is possible to consider the overall outage for all packets within the network in the confined area. Outage probability measures are defined for different system models and closed-form expressions for the outage are derived for the Individual Outage Probability (IOP), the Overall Outage Probability (OOP), the IOP for one packet (IOPP), and the OOP for all packets (OOPP), with and without the presence of attackers and/or strong interference. These reliability metrics can be adopted to analyze the effects of a wide range of parameters such as power allocation, node positions, the use of relay nodes or retransmissions, etc. on the individual link, individual source packet, and overall network reliability. The analysis thereby makes it possible to provide a set of general guidelines for tailoring the protocols and enhance the communication reliability of all legitimate nodes in the CPS. Having the closed-form expressions readily available also enables recalculating and adjusting parameters faster in order to find the best solution to improve the communication reliability during runtime. The thesis work demonstrates how outage probability can be used to enhance system performance in several example scenarios, including a multiple access scheme, pairwise Non-Orthogonal Multiple Access (NOMA), mobile access points and/or relay nodes. The outage analysis can thereby be applied to an existing CPS application to enhance reliability, robustness, and flexibility while maintaining a low delay.
Abstract

Some types of Cyber-Physical System (CPS) applications found within e.g., quarrying, mining, harbors, and construction sites, operate within confined areas. To guarantee that communications between nodes in such systems operate smoothly, the adopted wireless communication protocols must meet stringent requirements, even in the presence of interference and/or jamming. This thesis work targets finding performance metrics suitable for designing and evaluating wireless networks when used for CPSs in confined areas. Given the shortage of spectrum and the increased risk of cyber-attacks experienced lately, the protocols must also be adjusted to perform well when subject to strong interference and/or adversary jamming. Hence, to be useful in practice, metrics that can be recalculated during runtime are needed, such that they can be used not only to propose, select, and tailor the communication protocols to fulfill the stringent CPS requirements but also to optimize their performance during runtime. The literature survey conducted in this thesis shows that a reliability metric in terms of thresholding the so-called outage probability is valuable for all design steps as well as for continuously optimizing the communications. However, since the outage probability is defined as the probability that an individual wireless link will experience outage, it does not address the reliability of the entire network within the confined area. To this end, the thesis work shows that it is possible to consider overall outage probabilities and evaluate the probability of outage for each individual packet from a specific source node to a final destination, including all possible links in the network. This way, the overall outage for all packets within the network in the confined area can be assessed. Outage probability measures are defined for different system models and closed-form
expressions are derived for the Individual Outage Probability (IOP), the Overall Outage Probability (OOP), the IOP for one packet (IOPP), and the OOP for all packets (OOPP), with and without the presence of attackers and/or strong interference. These reliability metrics can be adopted to analyze the effects of a wide range of parameters such as power allocation, node positions, the use of relay nodes or retransmissions, etc. on the individual link, individual source packet, and overall network reliability. The analysis thereby makes it possible to provide a set of general guidelines for tailoring the protocols and enhance the communication reliability of all legitimate nodes in the CPS. Having the closed-form expressions readily available also enables recalculating and adjusting parameters faster in order to improve the communication reliability during runtime. The thesis work demonstrates how outage probability can be used to enhance system performance in several example scenarios, including a multiple access scheme, pairwise Non-Orthogonal Multiple Access (NOMA), mobile access points and/or relay nodes. The outage analysis can thereby be applied to an existing CPS application to enhance reliability, robustness, and flexibility while maintaining a low delay.
Sammanfattning


Litteraturundersökningen som genomförts i denna avhandling visar att ett tillförlitlighetsmått som använder tröskelvärden för den så kallade ”outage probability” (sannolikheten för avbrott i den trådlösa kommunikationen) är värdefullt för att utveckla såväl som för att kontinuerligt optimera kommunikationsprotokoll. Problemets numeriska storlek för avbrott definieras som sannolikheten att en enskild trådlös länk kommer att drabbas av ett avbrott. Det inbegriper alltså inte tillförlitligheten för hela nätverket inom det begränsade området. Avhandlingen visar att det är möjligt att formulera övergripande prestandamått som kan användas för att utvärdera sannolikheten för avbrott för varje enskilt
Acknowledgment

First, I wish to express my deepest appreciation to Elisabeth Uhlemann, my main supervisor, for her remarkable contributions to my academic journey. She has consistently demonstrated exceptional mentorship qualities, positioning her among the most exemplary supervisors worldwide. Additionally, I extend my gratitude to Le-Nam Hoang, whose engagement extends beyond scientific discussions, creating a sense of familiarity akin to my hometown in Sweden. Moreover, I am grateful to Svetlana Girs, my co-supervisor and boss, whose patience in rectifying numerous grammatical errors and other matters has been invaluable. The assistance provided by these individuals, encompassing unswerving patience, support, guidance, inspiration, encouragement, and guidance, has been indispensable in my successful navigation of the intricate doctoral journey and completion of my thesis. Lastly, I would like to acknowledge Hung Tran for his supervision during the initial stages of my PhD pursuit.

Second, I would like to thank Thomas Nolte for their valuable feedback on the PhD thesis. I also would like to thank the opponent and grading committee, Viktoria Fodor, Mats Bengtsson, Fredrik Brännström, Stefan Parkvall, and Jens Zander for their time and effort. I wish to express my appreciation to lecturers and professors from whom I learned a lot during courses, workshops, and summer schools.

Third, I want to thank colleagues from IDT, Data Communication groups, IDT administration staff, FORA members, discussion partners in Danish Technological Institute, IDT PhD students, especially, Václav Struhár, Salman Shaik, Shahriar Hasan, Nitin Desai, Zeinab Bakhshi Valojerdi, Taufik Akbar Sitompul, Björn Leander, and many more for your help, support, encouragement, and
discussion.

Last but not least, I am very thankful to my family, my parents, my parents-in-law, especially, my wife Phuong Chi Hoang, and my children Sofia Dao, Jenny Dao for their love.

This work has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 764785, FORA—Fog Computing for Robotics and Industrial Automation and from the Swedish Foundation for Strategic Research through the Serendipity Project.

Van-Lan Dao
Västerås, September, 2023
List of Publications

Papers included in this thesis

**Paper A:** Van-Lan Dao, Hung Tran, Svetlana Girs, Elisabeth Uhlemann, ”Reliability and fairness for UAV communication based on Non-Orthogonal Multiple Access”, *IEEE International Conference on Communications Workshops*, Shanghai, China, 2019, pp. 1-6.


**Paper E:** Van-Lan Dao, Svetlana Girs, Elisabeth Uhlemann, ”Defeating jamming attacks in downlink pairwise NOMA using relaying”, *IEEE International Conference on Communications Workshops*.

---

1The included papers have been reformatted to comply with the thesis layout.
Symposium on Personal, Indoor and Mobile Radio Communications, Toronto, ON, Canada, 2023 (accepted).


Related publications, not included in this thesis


Licentiate Thesis

## Contents

I Thesis  
1 Introduction 3  
  1.1 Cyber-Physical Systems ........................................... 6  
  1.2 Medium Access Control (MAC) ...................................... 8  
  1.3 Jamming Attacks and Interference .................................. 10  
  1.4 Main Players in a Confined Area ..................................... 11  
  1.5 Scope and Structure of the Thesis ................................... 13  

2 Research Overview 15  
  2.1 Research Goal and Research Questions .............................. 15  
  2.2 Research Method and Process ........................................ 16  
    2.2.1 Research Method ................................................. 16  
    2.2.2 Research Process ................................................ 17  

3 Performance Measures and Outage Probability 21  
  3.1 Performance Metrics and Interdependencies ......................... 21  
    3.1.1 Throughput ...................................................... 21  
    3.1.2 Reliability ...................................................... 22  
    3.1.3 Latency .......................................................... 23  
    3.1.4 Safety ............................................................ 23  
    3.1.5 Security .......................................................... 24  
    3.1.6 Power Consumption .............................................. 24  
    3.1.7 Complexity ...................................................... 25  
  3.2 Outage Probability .................................................... 25
## Research Results

### 4.1 Thesis Contributions

- C1: Literature survey and discussion on performance metrics for evaluating wireless links used for CPSs operating in confined areas
- C2: Defining the outage probability as a suitable metric for CPS networks in confined areas
- C3: Derived methods to obtain closed-form expressions of different outage probabilities on the link level, i.e., IOP, OOP, and on the network level IOPP and OOPP
- C4: Adopting the derived performance metrics to improve reliability by tailoring and selecting proper protocol settings
- C5: Using the OOP to adapt the location of mobile nodes in the CPS to enhance the reliability in the presence of a jamming attack
- C6: Using the IOPP and OOPP to select relay nodes to improve the reliability of CPS networks in confined areas in the presence of jamming attacks
- C7: Proposal of a framework for using pairwise NOMA in existing CPS to improve reliability performance while maintaining low delay
- C8: Formulation of guidelines for how to enhance the communication reliability for CPS applications in confined areas based on derived outage probabilities with and without the presence of attackers
- Validation

### 4.2 Overview of the Included Papers

- Personal Contributions
- Included Papers

Paper A: Reliability and Fairness for UAV Communication Based on Non-Orthogonal Multiple Access
Paper B: Outage Performance of Pairwise NOMA Allowing a Dynamic Decoding Order and Optimal Pairs of Power Levels ..... 36

Paper C: Defeating Jamming Using Outage Performance Aware Joint Power Allocation and Access Point Placement in Uplink Pairwise NOMA ..... 37

Paper D: Outage Performance Comparison of Adaptive Relaying Schemes Subject to Jamming ..... 38

Paper E: Defeating Jamming Attacks in Downlink Pairwise NOMA Using Relaying ..... 39

Paper F: Dealing with Jamming Attacks in Uplink Pairwise NOMA Using Outage Analysis, Smart Relaying and Redundant Transmissions ..... 40

Paper G: Anomaly Attack Detection in Wireless Networks Using DCNN ..... 41

5 Conclusion ..... 43
5.1 Future Work ..... 44

Bibliography ..... 45

II Included Papers ..... 55

6 Paper A: Reliability and Fairness for UAV Communication Based on Non-Orthogonal Multiple Access ..... 57
6.1 Introduction ..... 59
6.2 NOMA Concept ..... 60
6.3 Channel Model And Communication Protocol ..... 61
6.3.1 Channel Model ..... 62
6.3.2 Communication Protocol ..... 63
6.4 Optimization Algorithm For The UAV Altitude And User PAC ..... 65
6.5 Numerical Results ..... 67
6.6 Conclusions and Future Work ..... 73
6.7 Acknowledgements ........................................... 73
Bibliography ....................................................... 75

7 Paper B:
Outage Performance of Pairwise NOMA Allowing a Dynamic Decoding Order and Optimal Pairs of Power Levels 79

7.1 Introduction .................................................... 81
  7.1.1 Related Works ........................................... 83
  7.1.2 Motivations and Contributions ............................. 84
7.2 System Model ................................................... 85
7.3 Decoding Order And Power Allocation ......................... 87
  7.3.1 Downlink Pairwise NOMA ................................ 89
  7.3.2 Uplink Pairwise NOMA .................................... 90
  Fixed Pairwise Power Allocation ................................. 91
  Ideal Dynamic Power Allocation ................................. 92
7.4 Overall Outage Probability Analysis ............................ 92
  7.4.1 Downlink Pairwise NOMA ................................ 94
  7.4.2 Uplink Pairwise NOMA .................................... 97
  Fixed Pairwise Power Allocation ................................. 98
  Ideal Dynamic Power Allocation ................................. 101
7.5 Optimal Power Allocation .................................... 102
7.6 Numerical Results ............................................. 109
  7.6.1 Downlink Pairwise NOMA ................................ 109
  7.6.2 Uplink Pairwise NOMA .................................... 117
  7.6.3 Discussion ................................................ 123
7.7 Conclusion ..................................................... 126
7.8 APPENDIX ..................................................... 126
  7.8.1 Derivation of the Probability $p$ ............................ 126
  7.8.2 The First Derivative of $I_{1b}$, $I_{2b}$, $I_{3b}$, $I_{4b}$ with $m_1 = m_2 = 1$ .... 128
Bibliography ....................................................... 131
8 Paper C: Defeating Jamming Using Outage Performance Aware Joint Power Allocation and Access Point Placement in Uplink Pairwise NOMA 137
8.1 Introduction 139
8.2 System Model 143
8.3 Outage Performance Analysis 147
  8.3.1 Overall Outage Probability 147
  8.3.2 Individual Outage Probability 155
8.4 Joint Power Allocation and UAV Placement Design 157
  8.4.1 Scenario I: Fixed Jammer 158
  8.4.2 Scenario II: Mobile Jammer 165
  8.4.3 Complexity of the Proposed Algorithms 169
8.5 Numerical Results and Discussions 170
  8.5.1 Individual Outage Probability 171
  8.5.2 Overall Outage Probability 176
    Scenario I: Fixed Jammer 182
    Scenario II: Mobile Jammer 187
  8.5.3 Discussions 191
8.6 Conclusions 193
8.7 APPENDIX 193
  8.7.1 Proof of Lemma 1 195
  8.7.2 Proof of lemma 2 198
  8.7.3 Proof of lemma 3 198
Bibliography 199

9 Paper D: Outage Performance Comparison of Adaptive Relaying Schemes Subject to Jamming 207
9.1 Introduction 209
9.2 Related Works 210
9.3 System Model 211
9.4 Relay Selection and Outage Probability 213
  9.4.1 Group A: Relay selection based on channel gains 214
  9.4.2 Group B: Relay selection based on SINR 214
### Contents

9.4.3 Group C: Benchmarking RS schemes ................................. 215  
9.4.4 Outage Probability .................................................. 216  
9.5 Semi-analytical Setup .................................................. 216  
9.6 Results .................................................................. 218  
9.7 Discussions and Guidelines ............................................. 226  
9.8 Conclusion ............................................................... 229  
Bibliography ................................................................. 231  

#### 10 Paper E:  
**Defeating Jamming Attacks in Downlink Pairwise NOMA Using Relaying**  
10.1 Introduction .............................................................. 237  
10.2 System Model ............................................................ 239  
10.3 Outage Probability Analysis .......................................... 241  
10.4 Optimizing Power Allocation and Destination Pairing .......... 244  
10.5 Results ................................................................. 245  
10.6 Conclusion .............................................................. 251  
Bibliography ................................................................. 253  

#### 11 Paper F:  
**Dealing with Jamming Attacks in Uplink Pairwise NOMA Using Outage Analysis, Smart Relaying and Redundant Transmissions**  
11.1 Introduction .............................................................. 259  
11.2 Related Works ........................................................... 262  
11.3 System Model ............................................................ 263  
11.4 Protocols ................................................................ 267  
11.4.1 Conventional NOMA Relaying Protocol (CNRP) .......... 267  
11.4.2 Full NOMA Relaying Protocol (FNRP) ...................... 268  
11.4.3 Retransmission NOMA Protocol (RNP) ..................... 268  
11.4.4 Adaptive Power Allocation OMA Protocol (APAOP) .... 270  
11.5 Outage Performance Analysis ....................................... 270  
11.5.1 The IOP of each Source Node at the Relayer and the Destination in the First Phase ....................... 270  
11.5.2 The IOPs at the Destination When Using OMA .......... 273  
11.5.3 The IOP for one packet of each source node for the CNRP 274
Contents xvii

11.5.4 The IOP for one packet of each source node for the FNRP 275
11.5.5 The IOP for one packet of each source node for the RNP 275
11.5.6 Definition of OOPP ................................ 275
11.6 Dealing with Dynamic Conditions Using Deep Reinforcement Learning ................................ 276
11.7 Numerical Results ................................ 279
11.7.1 Guidelines ................................ 283
11.8 Conclusions ................................ 285
11.8.1 Appendix I ................................ 286
11.8.2 Appendix II ................................ 294
11.8.3 Appendix III ................................ 294
Bibliography ................................ 297

12 Paper G:
Anomaly Attack Detection in Wireless Networks Using DCNN 305
12.1 Introduction ................................ 307
12.2 Use Cases ................................ 309
12.2.1 Wireless Sensors in a Paper Mill ............. 309
12.2.2 Waste-Water Handling - Water Quality Measurements 310
12.3 System Model and Signature Measurement ........ 311
12.4 Deep Convolutional Neural network Design ....... 312
12.5 Results and Discussions ........................ 316
12.6 System Reaction ................................ 319
12.7 Conclusions ................................ 320
Bibliography ................................ 323
I

Thesis
Chapter 1

Introduction

With the latest developments in Industry 4.0, many companies are going through a change that aims to improve not only production, life cycles, and recycling of products and processes but also the quality of human life [1, 2]. The integration of production and information systems is realized in Industry 4.0 through connecting and connected Cyber-Physical Systems (CPSs), implying that the production mode is sometimes also shifted from centralized to decentralized cooperating systems. Connected and often also autonomous CPSs will be present in most industrial sectors and applications such as production technology, mechanical engineering, telemedicine, automation, the automotive industry, energy, and transportation systems. A CPS basically builds upon three key enablers: computing, communication, and control (including sensors, actuators, etc.) [3]. Communication, including both wired and wireless networks, plays a key role to ensure interaction both between different collaborating CPSs and in-between different parts of a CPS itself, i.e., between the computing entity representing the cyber part and the sensors and actuators interacting with the physical world [4]. A discussion regarding the differences between CPS and Internet of Things (IoT) is conducted in [5]. It is argued that the concept of CPS has emerged from a systems engineering and control perspective, whereas IoT has emerged from a networking and information technology perspective. A common denominator between both concepts is the strict requirements on real-time, reliability, and security, especially when applied in industrial applications [3, 6]. In addition,
strict requirements on safety and security are dictated for industrial applications by different standards such as IEC 62443, IEC 61508, and IEC 61784 [7, 8, 9].

Since all CPSs interact with their surrounding environment, timely actions are of the essence, and therefore, almost all CPSs have one or more deadlines to meet. This implies that the correct behavior of the CPSs not only depends on the correct output of the computing system but also when in time the output comes. Consequently, the computing system needs to prioritize different tasks according to the corresponding deadlines, and schedule its actions to ensure predictable and timely behavior. To meet real-time deadlines within the communication part of the CPSs, predictable and timely channel access as well as high-reliability play very crucial roles. Therefore, contention-free medium access control protocols such as Time Division Multiple Access (TDMA) are often used in industrial applications. With TDMA, predictable channel access can be guaranteed, and scheduling algorithms can be used to make sure access is granted to the most important communication task given the deadlines in the system. However, getting timely access to the channel does not necessarily ensure sufficient reliability. Therefore, retransmissions are typically used in industrial communication protocols. These are scheduled in a similar way, using the TDMA protocol so that a sufficient number of retransmissions can be made before the deadline, in order to ensure that the system meets the stipulated packet error rate. Therefore, when trying to enhance the performance of existing industrial systems, or adding one or more wireless links to an existing wired system, it is of great benefit if the changes comply with the TDMA protocol and existing schedulers to smoothen integration with already running systems and simplify further safety assurance procedures [10].

Currently, there is an increased interest in using wireless networks for a wide range of industrial applications due to a significant reduction of costs concerning deployment, implementation, maintenance, and flexibility compared to wired networks. Especially, systems consisting of mobile devices or rotating parts benefit from wireless connectivity. However, industrial environments often include lots of metallic clutter, moving machines, and robots, as well as processes emitting radio disturbances, which might result in bit errors, packet delays, and losses which in turn significantly affect the reliability of the wireless communication [11]. At the same time, industrial applications, e.g., factory or
process automation that include CPSs have stringent constraints on timeliness and reliability, e.g., packet error rate should be smaller than $10^{-6}$ for factory automation [3, 12]. Wireless systems must aim to fulfill these requirements with a sufficient level of predictability if they are to be used in safety-critical industrial systems [13].

It should be noted that wireless transmissions are more vulnerable to jamming and/or eavesdropping attacks due to the inherent open nature of the wireless communication channel [6, 14]. Since a jamming attack can interrupt or interfere with the ongoing legitimate transmissions by generating a noise signal present in all relevant channels, it causes problems with predictability even in cases where the reliability has been ensured through, e.g., pre-scheduled retransmissions. As an example, the National Institute of Standards and Technology (NIST) reported a detected vulnerability towards jamming attacks as follows: ”An issue was discovered on ABUS Secvest FUAA50000 3.01.01 devices. Due to an insufficient implementation of jamming detection, an attacker is able to suppress correctly received RF messages sent between wireless peripheral components, e.g., wireless detectors or remote controls, and the ABUS Secvest alarm central. An attacker is able to perform a 'reactive jamming' attack” [15]. Consequently, anti-jamming techniques and methods to mitigate problems with reliability in case of intentional or unintentional interference are also needed to ensure the predictable behavior of wireless systems used in industry.

A subset of CPSs found within mining, and quarrying or similar, operate in confined areas. This means that the considered CPS applications rely on fairly isolated communication systems located inside a border in the form of a fence or a wall in order to satisfy application safety and security requirements. The requirement for predictable communication and reliability is high for such applications. One or more wireless local area networks are typically formed to operate either independently or collaboratively to complete different tasks. When they operate independently, they can create interference. Therefore, it is important to consider both individual link reliability as well as overall network reliability within the confined area when proposing wireless protocols for these applications. In addition, potential attackers in terms of jammers and/or eavesdroppers may be present outside of the border. This means that wireless devices located close to the border can be subject to attackers located outside of
Chapter 1. Introduction

the border. This should be taken into account when designing wireless protocols for CPSs within confined areas.

1.1 Cyber-Physical Systems

In industrial applications, such as quarrying, mining, construction sites, road work, forestry, etc. [16], connected mobile robots/vehicles form different clusters and collaborate with each other; often, following, e.g., the Lean method [17], to improve the productivity, Figure 1.1. Each cluster includes a number of nodes collaborating with each other to complete different sub-tasks. Different clusters may be responsible for independent sub-tasks and thereby do not necessarily need to communicate with each other. All nodes within each cluster could work as source nodes, destinations, relayers, and/or friendly jammers. Due to the temporary and mobile characteristics of these applications, all devices should be easily deployed to collaborate with each other as well as easily moved or removed using a minimum of infrastructure. These applications usually operate in confined areas to ensure safety and security requirements. Attackers in terms of jammers and/or eavesdroppers may, however, be present, but in this thesis work, it is assumed that they are located outside of the physical border. The legitimate wireless systems located within the confined area must guarantee that all legitimate applications operate smoothly even in the presence of attackers and/or interferers.

Trustworthiness is of high importance for a CPS [5]. Due to the interaction between the physical world and the computing world, the requirements entail all of the following to enable trustworthiness:

- Reliability: Depending on each specific application, packet losses can cause more or less serious problems such as economic loss or safety problems at the system level due to, e.g., stopping of the production chain. Therefore, reliable systems with low error probability are sought.

- Meeting real-time deadlines: In practice, if the transmitted packets do not reach their destinations before the deadline, problems with safety and functionality may occur. Timely delivery of data is therefore a functional
requirement for CPS. As a result, the applications must meet real-time deadlines to avoid failures of the application.

- **Security**: As mentioned above, wireless links have an open nature, vulnerable to being attacked by jamming and/or eavesdropping [6, 14]. It is noted that while eavesdropping attacks may be addressed by using encryption algorithms, interference and/or jamming attacks may influence communication reliability significantly [18]. As a result, anti-jamming solutions should be included already when designing wireless protocols.

- **Safety**: To guarantee that the system always works as intended and if some parts of it breaks down, it does so without causing damages/accidents for infrastructure, environment, and humans, safety is a strict requirement in industry [19, 20].

- **Heterogeneity**: Industrial networks have developed significantly over the years and a wide range of wired and/or wireless technologies have been used. This implies that network heterogeneity is a requirement in industry [21]. Thus, new wireless protocols should be compatible with
existing networks as well as future industrial networks. Further, since more and more devices connect, the networks should also be able to handle mixed-criticality requirements [22] and provide user fairness given the specific requirements of each connected device.

There are several wireless standards, i.e., Wireless Highway Addressable Remote Transducer (WirelessHART) [23], ISA 100.11a [24], Wireless Interface for Sensors and Actuators (WISA) from ABB [25], real-time WiFi [26], Wireless Networks for Industrial Automation - Factory Automation (WIA-FA) [27], Industrial Wireless Local Area Network (IWLAN) by Siemens [28], all of which have been proposed to be used in industrial applications. Most of them build upon IEEE 802.11 and IEEE 802.15 [29] but use a TDMA scheme on top of the existing Medium Access Control (MAC) layer. Wireless HART and ISA 100.11a are designed mainly for industrial applications, but also for, e.g., condition monitoring, which has quite relaxed requirements on latency and real-time [30, 31]. WirelessHART can guarantee reliable communications but does not cope well with packet losses [32]. On the other hand, WISA has been designed to fulfill the requirements of fast and reliable communication for industrial applications with an end-to-end latency of less than 20 ms [11, 12]. However, both WirelessHART and WISA are based on the physical layer of IEEE 802.15, which was designed for low-power and limited data rate communication, meaning that they only support low scalability within a specific cycle time [33]. In order to increase the data rate, IEEE 802.11 WLAN has been proposed, to support higher data rates enabling performance figures in the same order of magnitude as industrial wired networks [34]. Accordingly, real-time WiFi and WIA-FA are both based on IEEE 802.11 and use TDMA to provide a deterministic timing guarantee on packet delivery and short cycle time.

1.2 Medium Access Control (MAC)

The MAC layer is responsible for channel access to a shared medium within a local area network. One of the biggest problems for the MAC layer is to handle massive connections from devices, while maintaining the required quality of service, e.g., a certain latency or reliability level, for each device has to be maintained. Thus, many MAC protocols have been proposed which can be grouped
into three main categories: contention-based MAC protocols, contention-free MAC protocols, and hybrid MAC protocols. Each category has different advantages and disadvantages as follows [35]:

- For contention-based protocols: The principle of the protocols belonging to this group is that all nodes contend for the channel to acquire access and send data in different ways, e.g., ALOHA, Carrier Sense Multiple Access (CSMA). When the number of source nodes is small, these protocols are very effective. However, the collision probability among source nodes wanting to transmit simultaneously at the same time-frequency instance increases significantly for high network loads, leading to a growth of the channel access delay, or a reduction in reliability.

- Contention-free protocols: These protocols remove the biggest drawback of contention-based protocols due to each source node being assigned a part of the shared resources, e.g., a time slot in TDMA, a frequency in Frequency Division Multiple Access (FDMA), etc. Typically, each share of the resources has to be orthogonal to the others, leading to a strict upper limit on the number of available shares. However, the protocols in this category are not very flexible with respect to a varying number of (mobile) nodes or dynamic network conditions. Furthermore, the effectiveness is rather low for lightly or unevenly loaded networks. In contrast, for high network loads, the channel utilization of the contention-free protocols is better.

- Hybrid MAC protocols: As can be concluded from the above reasoning, contention-based MAC protocols are more effective for low loads. In contrast, when the number of source nodes increases dramatically with higher loads, contention-free MAC protocols are more suitable. Hence, hybrid MAC protocols are proposed to have both benefits from the two MAC protocols above, e.g., TDMA-CSMA, Code Division Multiple Access (CDMA)-CSMA, FDMA-CSMA.

All aforementioned MACs are orthogonal MACs and all aim to avoid collisions among wireless devices or reduce the probability of collision to improve the communication reliability. Recently, Non-Orthogonal Multiple Access (NOMA)
has emerged as a promising technique offering low latency, high throughput, and predictable channel access [36, 37]. The main principle of NOMA is to remove the requirement of orthogonality between the different users so that multiple users can be served simultaneously by sharing the same, often limited, system resources. The superior spectral efficiency of NOMA helps reduce the latency of communication is shown in [38]. In other words, multiple nodes are served simultaneously using the same time-frequency resources but different power levels. To separate the signals, successive Interference Cancellation (SIC) is used at the receiver. It has been shown that if set up accordingly, NOMA could outperform traditional multiple access schemes, e.g., TDMA, for both uplink and downlink in terms of throughput and reliability for the critical-service users [37, 39]. However, NOMA could also be used on top of an existing TDMA scheme to enhance the performance of an existing CPSs, while providing backwards compatibility [36]. Moreover, NOMA could easily switch back to an ordinary TDMA scheme simply by assigning all power to one user, and zero to the others, if and when needed.

It should be noted, however, that the SIC process is a complex operation and becomes even more complicated with an increased number of users. Therefore, to reduce the complexity as well as the cost of the receivers, the number of active users at the same time slot with NOMA should not be too large [40]. Due to this practical constraint, many previous papers have evaluated the performance of pairwise NOMA, i.e., NOMA in which, at each time-frequency instance, only two users are transmitting simultaneously to an Access Point (AP) or alternatively receiving a superimposed signal from the AP [41, 37, 42]. In particular, if the main purpose of using NOMA is to enhance the performance of an existing TDMA scheme, tailoring pairwise NOMA to be used on top of TDMA to ensure timely and predictable channel assess with higher reliability is of high practical interest to many industrial systems.

1.3 Jamming Attacks and Interference

When considering a scenario within a confined area, in which multiple legitimate nodes are operating inside the border, we assume that attackers are only allowed to be placed outside of the border. However, due to the open nature of wire-
less networks, wireless devices, including malicious eavesdroppers, operating at the same frequency band within communication range, can overhear and may correctly decode transmitted messages [6]. Similarly, a harmful jammer can transmit a jamming signal over all relevant channels to attack the legal communication system [6, 14] causing them to, e.g., miss deadlines or waste power. A collaboration between an eavesdropper and a jammer can make the attack smarter, e.g., being able to detect a legitimate active transmission and trigger a reactive jammer [15]. Hence, an important requirement for future CPSs is to include security in terms of, e.g., mechanisms to defeat jamming and/or eavesdropping attacks to ensure that the system can operate smoothly, even in the presence of cyber-attacks. To do this, a friendly jammer could for example be deployed to defeat an eavesdropping attack [43].

Co-located clusters may also cause strong interference to one another [18]. Also other wireless devices operating at adjacent frequency bands can sometimes create interference. As it is predicted that the number of connected devices will increase significantly in the future, we may experience a situation where spectrum reuse and dense deployment are unavoidable [44]. As a result, interference management must be considered [45, 46, 47], and, more importantly, the system models must take attacks in terms of any type of interference and/or malicious jamming into account.

1.4 Main Players in a Confined Area

As discussed in Subsection 1.3, potential eavesdroppers and/or jammers can attack the legitimate communication systems inside the confined area. In the literature, the system models usually consider jamming as noise or interference from other communication systems. In this thesis, a general system model including potential jammers is adopted and strategies to defend the legitimate systems is instituted, Figure 1.2. Accordingly, the main players of the system model are as follows:

- Legitimate nodes: In general, all nodes can be source nodes, destinations, and/or relayers. Relaying strategies may be employed when: (i) the distance between source nodes and destinations is far enough, a deep
fade is likely to occur or when nodes are subject to jamming; (ii) the transmitted packets are short, while the timing requirement is strict, and thus packet aggregation and/or source relaying can be adopted [48]. The legitimate models can deploy several strategies such as adjusting node positions, power allocation, relay selection, and so on depending on the specific protocols.

- Attacker nodes: Attacker nodes that are considered in this work are smart jammers, which may aim to disturb the legitimate communication, e.g., by forcing nodes to miss deadlines, while staying hidden from the detection techniques of the legal systems. The potential strategies for the attackers can be adjusting their positions and transmitting power depending on their available resources.

![Figure 1.2. System model.](image)

It is realized that the benefits of legitimate communication systems and
attacker systems conflict completely with each other. Therefore, game theory is a tool used in this thesis.

1.5 Scope and Structure of the Thesis

This thesis work targets finding performance metrics suitable for designing as well as evaluating wireless networks when used for CPSs in confined areas. A review of appropriate performance metrics to evaluate wireless networks of CPSs is therefore first conducted. Second, outage probabilities are concluded to be suitable as performance metric for the considered type of systems. Third, methods to calculate closed-form expressions for each type of outage probability are presented. After that, the outage probabilities are used to optimize and tailor the communication protocols in various scenarios with and without the presence of an attacker in terms of jamming and/or eavesdropping. Finally, general design guidelines for wireless networks used for the considered CPS applications in confined areas are provided.

The thesis is divided into two main parts. Part I is an overview of the thesis, while Part II is a collection of the included papers. Part I starts with Chapter 1 presenting the motivation for the thesis. Next, Chapter 2 presents the overall research questions and the research methodology. An overview of relevant performance measures for CPSs in confined areas is provided in Chapter 3, after which the thesis contributions together with an overview of the included papers, are summarized in Chapter 4. Finally, Chapter 5 concludes the first part of the thesis and outlines the future work.
Chapter 2

Research Overview

2.1 Research Goal and Research Questions

The main goal of this thesis work is to identify and derive performance metrics which are suitable for designing, evaluating and continuously improving the performance of CPS when used within confined areas.

Due to the characteristics of CPS applications, different groups of wireless devices can work independently or collaboratively depending on their specific tasks. However, most performance metrics that have been proposed in the literature so far are targeting centralized networks. Distributed networks or multiple co-located clusters operating jointly or separately within the same area, require a different approach. Moreover, many performance measures target maximizing the throughput or the spectral efficiency. The CPSs requirement on high reliability and timeliness is not guaranteed by a high average throughput. In fact, CPSs can work well with a relatively low average throughput as long as the worst case is good enough, i.e., the signal-to-interference-plus-noise ratio is above a certain threshold. Similarly, spectral efficiency aims to fit many users into the same time-frequency space, while in CPSs, all redundant best-effort users and transmissions are removed to guarantee that the worst case is above the threshold.

To this end, suitable performance metrics for CPS in industrial applications are needed. Further, these metrics need to be derived such that they entail the
entire network within the confined area. Finally, low complexity methods are needed to propose, select, optimize, and/or tailor the communication protocols such that they fulfill the requirements of CPS with and without the presence of an attacker in terms of jamming and/or interference.

To obtain the main goal of this thesis, four research questions are formulated:

• **RQ1:** Which metrics are suitable to evaluate the performance of a wireless link when used by a CPS?

• **RQ2:** Given the link metrics, how to define metrics which enable evaluating the performance of the entire CPS network deployed in a confined area?

• **RQ3:** How to use the derived performance metrics to propose, select or optimize communication protocols as well as tailor and select proper settings for these protocols such that they are suited for the fading channels encountered in the considered applications both with and without the presence of a jamming attack?

• **RQ4:** Given the complexity constraints and the performance improvements gained, how to provide more general guidelines for online and offline selection of network topologies and wireless protocols for CPS in confined areas when interference comes from both co-located clusters and the presence of a jammer?

### 2.2 Research Method and Process

#### 2.2.1 Research Method

To derive the closed-form expressions for the performance metrics used in this thesis, a wide range of equations in [49] was used. However, it is not straightforward to directly apply the equations in [49] in various scenarios in [50, 51], and therefore Venn diagrams were adopted to divide the original problems into subcases before obtaining the derived performance metric. To check the correctness of the calculations, a semi-analytical method as presented
in Paper D was used. Moreover, in the presence of a jamming attack, a game theory method was used to describe the reactions of both players for a non-cooperative game before getting the Nash equilibrium points [51]. In addition, to find the optimal solutions for the considered system, various tools such as metaheuristic optimization and machine learning are applied in Papers C, E, F, and G, considering also their complexities.

2.2.2 Research Process

This thesis employs the hypothetico-deductive method, and the research process adheres to the sequential steps depicted in Figure 2.1 [52, 53].

- **Literature survey**: In this phase, a comprehensive compilation of publications pertaining to the thesis topic is created, followed by a meticulous review of a selected subset of relevant literature.

- **Identifying a list of problems**: The identification of emerging issues stems from the initial step as well as through dialogues with industrial collaboration partners. Subsequently, the problems are refined and narrowed down, leading to a specific focus on e.g., enhancing communication reliability and minimizing latency through the utilization of pairwise NOMA. The outcome of this phase is a compiled list of problems that, when resolved, have the potential to yield performance enhancements.

- **Select and formulate a problem**: Based on the outcomes of the preceding stage, a specific problem is selected for clarification and formulation in this subsequent step.

- **Literature review**: In this phase, the collected publications are revisited and thoroughly examined to gain a deeper comprehension of the problem. These papers serve as valuable resources for conducting a comparative analysis between the proposed solution and existing alternatives during the results analysis stage. Additionally, this step may generate novel suggestions for alternative solutions.

- **Propose a solution**: A novel solution is introduced to address the limitations identified in prior studies and/or enhance system performance in
comparison to both current industry practices and relevant research.

- Results collection and analysis: The proposed solution utilizes various tools such as Matlab, Mathematica, convex optimization, metaheuristic optimization, and machine learning. During the analysis phase, the results are compared with computer simulations to evaluate the effectiveness of the proposed solution in comparison to the current state-of-the-art. Based on the analysis, the following decisions can be made: (i) If the desired results are achieved, the possibility of an upgraded solution that can further improve system performance is considered. If available, the process goes back to the fifth step; otherwise, a new process starts from the third step. (ii) If the obtained results are unsatisfactory or do not meet expectations, the reasons are investigated, and the problem is reformulated to continue from the fourth step.
2.2 Research Method and Process

Identifying a list of problems
Reformulate the problem
Propose a solution
Results collection
Expected results?
Yes
No
Literature survey
Select and formulate a problem
Literature review
Propose a solution
Results collection
Results analysis
Explain why
Suggest new solution?
Yes
No
Expected results?
Figure 2.1. Research process.
Chapter 3

Performance Measures and Outage Probability

3.1 Performance Metrics and Interdependencies

In this Section, typical performance metrics are reviewed and then analyzed in terms of suitability for various applications.

3.1.1 Throughput

The achievable throughput or data rate between a pair of transmitter and receiver is defined as $R = \log_2(1 + \gamma)$, where $\gamma$ is the received Signal-to-Noise Ratio (SNR)/Signal-to-Interference-plus-Noise Ratio (SINR) at the receiver. There are two main goals related to the achievable rates in a multiple nodes scenario [54]:

- Maximize the total achievable data rates in uplink/downlink.
- Maximize the minimum data rate among the achievable data rates in uplink/downlink.

Moreover, there are several possible constraints such as maximum total transmit power at the Base Station (BS) or maximum transmit power at each source node and successful decoding at the receiver related to SNR/SINR, e.g., $\gamma \geq \gamma_0$. The aforementioned problems can be evaluated using [55].
This performance metric is suitable for various applications using centralized network topologies such as telecommunications when data packets are very long, e.g., packets containing video, image, music, voice, and similar data. For centralized networks, all tasks are scheduled and synchronized at the BS. However, industrial applications use both centralized and decentralized networks but usually exchange very short packets, while the reliability requirement is very high. Moreover, ad-hoc is a suitable network topology for industrial networks as it does not require deploying BSs. In addition, as mentioned in Subsection 1.1 most industrial wireless standards are based on IEEE 802.15.4 and thus operate at quite low data rates, e.g., 250 kps. More importantly, a high throughput says more about the average behaviour, and very little about timeliness, variance and reliability for a single packet. Therefore, this performance metric is not considered in this thesis.

3.1.2 Reliability

Due to the random nature of wireless channels, communication reliability in wireless networks is defined as a percentage of the transmitted packets that are delivered correctly to the receiver during a certain duration of time [38, 19]. A large number of factors such as transmit power, path loss, multipath fading, types of error-correcting codes, types of modulation, system bandwidth, length of the packet, etc., influence communication reliability. Therefore, many reliability metrics have been developed to evaluate the communication reliability of wireless networks, including outage probability, packet error rate, bit error rate, symbol error rate, and so on. Each reliability metric has its own advantages and disadvantages. The obtained reliability metrics for different scenarios can help to optimize the system resources and tailor the proposed protocols with appropriate settings while maintaining the given requirements. It is noted that the communication reliability in industrial applications is very stringent, for example, the packet error rate should not exceed $10^{-9}$ for the power electronics control and power system protection applications [12]. Therefore, reliability is a metric which is suitable for the considered systems.
3.1.3 Latency

In the literature, several terms for latency such as end-to-end latency, MAC-to-MAC latency, etc are introduced [56, 57, 58, 38]. In general, the latency is defined from the time a packet is available at the transmitter until this packet is decoded correctly at the receiver. Therefore, a wide range of factors affect the latency, including processing time at transceivers, encryption/decryption time, transmission time, guard time, re-transmission time, and so on. All packets should be delivered to the respective destinations before their deadlines in terms of the number of time slots. Therefore, latency or reliability as a function of time is one of the most important metrics in industry. Hence, this performance metric is suitable for the systems considered in this thesis and is expressed as e.g., a certain number of available time slots.

3.1.4 Safety

Safety is defined as the absence of catastrophic consequences on humans, infrastructure, and the environment [19]. For example, whenever an autonomous/automated vehicle detects any hazard/obstacle/accident, an emergency packet should be broadcasted over wireless channels to other vehicles and infrastructure. These packets should be delivered to the following vehicles and infrastructure in time with the highest reliability to avoid unexpected results. To meet a safety instrumented function, the design, application procedures, deployment methods, and maintenance methods of automatic protection systems are depicted in safety standards. There are two main families of safety standards, including one covering specific industrial sectors and another one covering industrial communications. The standards IEC 61508, IEC 61511, IEC 62061, ISO 26262, and EN 50126 are dedicated to all industries, automation processes, machinery, automotive, and railway industry, respectively. With the standard IEC 61508 for industrial scenarios, the probability of a failure should be smaller than, e.g., $2 \times 10^{-15}$ for a Safety Integrity Level 3 [20]. Therefore, reliability is still the key performance metric to guarantee safety requirements.
3.1.5 Security

A wide range of attacks in terms of jamming and/or eavesdropping are possible in wireless networks [6, 59, 60]. A jammer aims to generate the noise signal over relevant wireless channels, while the legitimate wireless communication system tries to remove these signals first before decoding its own useful signals by considering the residual noise as interference. Many techniques and strategies have been used to enhance communication reliability using various reliability metrics as discussed above. Eavesdropping attacks are very difficult to detect if they are passive. However, eavesdroppers also need to communicate with their own system, e.g., they can provide correct parts of packets for the jammers to make them smarter. Also, they can provide the estimated locations of the legitimated nodes and information on related packets. Consequently, the legitimate wireless system can still detect active eavesdroppers. To mitigate the eavesdropping attacks, many protocols have been proposed to reduce the information leakage probability [61, 62]. In other words, the proposed strategies try to significantly reduce the communication reliability in terms of the information leakage probability at the eavesdroppers. As a result, reliability metrics are still adopted to defeat both jamming and/or eavesdropping attacks. In fact, security and safety are related to each other, e.g., a connected safety-critical system is not safe if it is not secure [63]. Thereby, both security and safety can be evaluated by using reliability metrics. In industrial sectors, IEC 62443 standard can cover most industrial applications [64, 65].

3.1.6 Power Consumption

Power consumption is also a crucial performance metric when wireless devices operate in dangerous or inconvenient environments, in order not to have to change the battery frequently. To ensure that industrial applications operate smoothly and safely, the power supply systems are designed to guarantee the necessary budget for the whole system. Therefore, the problem here is how to meet the strict requirements on timeliness and reliability with the available power budget to guarantee the safety and security requirements. This metric is not considered specifically in the thesis as the criticality of the CPSs and the requirement on timeliness takes precedence over power. It is considered
implicitly by e.g., adapting the power allocation given a fixed power budget.

### 3.1.7 Complexity

A wide range of solutions has been proposed to maximize the selected performance metrics, e.g., communication reliability, based on available resources in terms of computing resources, power budget, system bandwidth, etc. However, several key resources are often limited in CPSs operating in confined areas, e.g., resources such as power budget and computing power, while the timing requirement is very stringent. Therefore, a trade-off between communication protocols and system performances should be taken into account. Moreover, optimization solutions also need to be considered for their worth. This means whether or not the obtained optimal solutions can gain much compared to simpler solutions, e.g., intuitive or random solutions. In the cases of stringent timeliness requirements, suboptimal solutions can also be used, e.g., using metaheuristic algorithms. This metric is taken into account when formulating closed form expressions and using machine learning to optimize performance as these methods lead to reduced complexity.

### 3.2 Outage Probability

Outage probability is the probability that the received SINR is smaller than a SINR threshold [66]. When this happen, it means that the current communication rate is not supported, and an outage is experienced. This outage is related to the reliability and it is a worst case measure, which is much more relevant than the average measure throughput. However, the outage probability is defined as the probability that one wireless link will experience outage. In other words, it estimates the quality of the individual link and not the entire network in the confined area. In this thesis work, several different outage probability measures are defined as seen in Figure 3.1. First, the Individual Outage Probability (IOP) considers only one direct link between the source node and the destination, Cluster 1 in Figure 3.1. When multiple source nodes communicate with a destination, the Overall Outage Probability (OOP) is useful to optimize the outage probabilities for the whole cluster, Cluster 2 in Figure 3.1. We note that
Figure 3.1. Reliability metrics in terms of outage probabilities.

A source packet can be delivered correctly to the destination via multiple links, e.g., when relayers are deployed. In this case, the IOP for one packet (IOPP) is useful as it evaluates the outage probability for one source packet and takes all possible links to the destination into account, Cluster 3 in Figure 3.1. Finally, the overall outage probability for all packets (OOPP) is needed to optimize the whole network when multiple source node packets and multiple relayers are employed, Cluster n in Figure 3.1. In this thesis work, all four measures are investigated for both Orthogonal Multiple Access (OMA) and pairwise NOMA.
Chapter 4

Research Results

In this Chapter, the research results and contributions are outlined. First, the overall contributions of the thesis are presented and then specific contributions of each of the seven included papers are highlighted.

4.1 Thesis Contributions

There is a wide range of performance metrics evaluating a single wireless link between a source and a destination. Therefore, an investigation into which metrics that are suitable for CPS applications with stringent requirements on timeliness and reliability, was made. The literature survey conducted in this thesis shows that a reliability metric in terms of thresholding the outage probability is valuable for all design steps: proposing, tailoring, optimizing, and ultimately selecting a good communication protocol. However, the outage probability is defined as the probability that one wireless link will experience outage. In other words, it estimates the quality of the individual link and not the entire network in the confined area. To this end, the thesis shows that it is possible to define and derive overall outage probabilities for the entire network, the individual clusters within the confined area and the individual source nodes. Outage probability measures are defined for different system models, with and without relay nodes and jammers, and closed-form expressions are derived for the Individual Outage Probability (IOP), the Overall Outage Probability (OOP), the IOP for one packet
(IOPP), and the overall outage probability for all packets (OOPP). These outage probabilities can be adopted to analyze the effects of a wide range of parameters such as power allocation, node positions, the use of relay nodes, etc. on the individual link, individual source packet, and overall network reliability. The analysis thereby makes it possible to provide a set of general guidelines for tailoring the protocols and enhancing the communication reliability of all legitimate nodes in the CPS. Having the closed-form expressions readily available also enables recalculating and adjusting parameters fast to find the best solution to improve the communication reliability during runtime. Finally, it is shown how outage probability can be used to propose changes to enhance system performance in an example scenario, where pairwise Non-Orthogonal Multiple Access (NOMA) and relaying are applied to an existing CPS application to enhance reliability, robustness, and flexibility while maintaining a low delay.

Consequently, the following research contributions have been made:

• C1: Literature survey and discussion on performance metrics for evaluating the quality of wireless links used for CPSs operating in confined areas.

• C2: Defining the outage probability as a suitable metric for CPS networks in confined areas.

• C3: Deriving methods to obtain closed-form expressions of different outage probabilities on the link level, i.e., IOP, OOP, and on the network level IOPP and OOPP when considering several hops, links, and paths.

• C4: Adopting the derived performance metrics to improve reliability by tailoring parameters and selecting appropriate protocol settings.

• C5: Using the outage probability for online adjustments of the location of mobile nodes to enhance the reliability of CPS in confined areas when subject to jamming.

• C6: Using the outage probability to select relay nodes to improve the reliability of CPS networks in confined areas in the presence of jamming attacks.
4.1 Thesis Contributions

- C7: Proposing a framework for using pairwise NOMA in existing CPSs to improve the reliability while maintaining a stipulated low delay.

- C8: Formulating guidelines for how to enhance the communication reliability for CPS applications in confined areas using the derived outage probabilities both with and without the presence of jammers and/or interferers.

A mapping of the contributions to the research questions is shown in Table 4.1. The first two contributions, the literature survey and identifying outage probability, C1 and C2, fulfill the first research question. In order to continue improving communication reliability, all possible links between a source node and a destination, e.g., also including potential relayers, should be deployed. Further, to adapt to dynamic environments, e.g., jammers’ positions and transmit power levels, the selected performance metrics should be recalculated fast to select proper settings. Hence C2 and C3 are provided to satisfy the second research question. When the closed-form expressions of the suitable performance metrics for both single links and multiple links are derived, contributions C4, C5, and C7 are made by employing the performance metrics to find a better solution, e.g., power allocation for each source node and relayer position also when jamming is considered. This satisfies the third research question. However, the complexity and performance of each protocol differ. Therefore, when analyzing different protocols, both the complexity and the performance gained should be taken into account. Selecting a less complex protocol with performance close to the best protocol but with much higher complexity is considered when providing useful guidelines. This is carried out by contributions C5, C6, C7, and C8 to address the fourth and last research question.

4.1.1 C1: Literature survey and discussion on performance metrics for evaluating wireless links used for CPSs operating in confined areas

A literature survey regarding different performance metrics for wireless networks such as throughput, latency, reliability, safety, security, power consumption, and complexity is conducted. Furthermore, the interdependencies of these performance metrics are discussed. Moreover, the purpose of each performance metric
Table 4.1. Mapping of contributions to research questions.

<table>
<thead>
<tr>
<th></th>
<th>RQ1</th>
<th>RQ2</th>
<th>RQ3</th>
<th>RQ4</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>C5</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>C6</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>C7</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C8</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

and its potential to evaluate CPS applications are also presented. The obtained results show that the reliability metric is both suitable and important. In particular, reliability as a function of time, i.e., the number of time slots should be assessed for CPS applications in confined areas. This is because when reliability performance is guaranteed, the legitimate wireless communication system can work well even in the presence of strong interferers and/or attackers. Moreover, both security and safety requirements can be transferred to the reliability requirement. Finally, the reliability metric outage probability as a function of a number of time slots is concluded to be an excellent performance metric for evaluating wireless links in CPS in confined areas.

4.1.2 C2: Defining the outage probability as a suitable metric for CPS networks in confined areas

The outage probability in terms of IOP, OOP, IOPP, and OOPP are defined for various scenarios with and without the presence of jamming attacks in confined areas. The outage probability allows for evaluating both individual link reliability, packet reliability, and the overall wireless network. Here, the IOP is to evaluate the communication reliability for each source node to the destination via one hop, while the IOPP takes multiple hops into consideration. Both IOP and IOPP can help to design communication protocols to meet the reliability requirement for different tasks such as critical tasks and best-effort
4.1 Thesis Contributions

When considering a network or a multiple clusters scenario, the OOP and OOPP are useful to optimize the overall wireless network performance, for example, to guarantee a fairness condition among all nodes. Note that the Overall IOP (OIOP) in Paper [67] and the OOPP are the same.

4.1.3 C3: Derived methods to obtain closed-form expressions of different outage probabilities on the link level, i.e., IOP, OOP, and on the network level IOPP and OOPP

When the channel models include fading, the channel gains are random variables (RVs). Removing these RVs from the outage probabilities is a way to obtain the closed-form expressions of IOP, OOP, IOPP, and OOPP. This is needed both for the analysis and for the optimization algorithms to guarantee that the best solution can be found fast enough. By using the Venn diagram method, closed-form expressions of the considered outage probabilities in different contexts with and without interferers and/or attackers were derived. These outage probabilities are useful to analyze the effects of many parameters on communication reliability.

4.1.4 C4: Adopting the derived performance metrics to improve reliability by tailoring and selecting proper protocol settings

By adopting the closed-form expression of the OOP, it was possible to optimize, tailor, and select proper protocol settings. Moreover, the outage probabilities are functions of a number of parameters such as power allocation, positions, and so on. This can help to understand how each parameter affects communication reliability when designing protocols. In other words, using the OOP to e.g., adjust the power allocation and selecting a better decoding order in a NOMA system was shown to not only improve the communication reliability but also reduce the complexity and computational load at the destination.
4.1.5 C5: Using the OOP to adapt the location of mobile nodes in the CPS to enhance the reliability in the presence of a jamming attack

When subject to a jamming attack, ensuring the reliability requirement in practice is very challenging. Moreover, the jammer can be mobile and smart enough to choose the best strategy for defeating the legitimate communication system. Therefore, the legal wireless communication system should recognize the situation and adapt. By using the closed-form expression of the OOP in the presence of a jammer, a non-cooperative game is formulated to model the potential reactions among all players (mobile access point and mobile jammer) to find the optimal strategy for each player in different scenarios. This is applied in confined areas, in which jammers are only allowed to be appeared outside of the border. When the Nash equilibrium points are obtained, all player requirements are satisfied. An analysis on how each parameter is affecting the communication reliability in terms of the derived OOP is also conducted, which can help narrow the search space for the proposed algorithms. This can help to find the best solution faster.

4.1.6 C6: Using the IOPP and OOPP to select relay nodes to improve the reliability of CPS networks in confined areas in the presence of jamming attacks

When interferers and/or jammers exist, communication protocols based on relaying strategies and re-transmission are analyzed. Different relay selection and re-transmission strategies are considered and evaluated to improve the communication reliability for legitimate nodes in a CPS. An intensive analysis of relay selection, power allocation, and user pairing affecting the communication reliability in terms of the closed-form expressions of OOPP is conducted. Moreover, a method using deep Reinforcement Learning (RL) to deal with uncertainty related to jammers’ positions and transmit power is introduced by using the OOPP as the reward function.
4.1 Thesis Contributions

4.1.7 C7: Proposal of a framework for using pairwise NOMA in existing CPS to improve reliability performance while maintaining low delay

Given the new tools in terms of outage probabilities, existing CPS can be made better, as in the selected use case. A use case with a mobile access point, like a Unmanned Aerial Vehicle (UAV) communicating with two robots using pairwise NOMA is considered, e.g., an autonomous garbage collection application supported by a UAV and two autonomous robots. Since a UAV is used, Line of Sight (LoS) channels can be adopted and hence, the decoding order used to extract the signal at each robot is decided simply based on the distance between the UAV and each robot. Moreover, the power allocation for the two users is found following the user fairness condition. This provides a framework on how to set up pairwise NOMA so that it fits the CPS which includes a UAV and two robots. The framework as such satisfies the main goal since the performance metric is selected based on CPS applications in confined areas. For more complex types of channel models including fading and jamming, the decoding order also needs to be adjusted as was done. Similarly, given different types of CPS, the power allocation could be tailored to achieve user fairness or to prioritize critical data traffic.

4.1.8 C8: Formulation of guidelines for how to enhance the communication reliability for CPS applications in confined areas based on derived outage probabilities with and without the presence of attackers

When the legitimate wireless system is attacked by a jamming entity, several guidelines in terms of power allocation for each node, user pairing, and UAV or mobile access point placement to improve communication reliability are provided. Moreover, a useful guideline to select the best relay selection is presented in the presence of jamming attacks. For legitimate communication systems, they should detect anomaly nodes in terms of jammers and eavesdroppers located outside of the border as soon as possible to deal with these. To this end, a solution for finding optimal hyperparameters for the designed neural network is provided. By determining exactly what interference from interferers or jammers
can be expected, the legitimate nodes can adapt their behavior to improve communication reliability. Moreover, how the systems should react to a detected rogue device, considering the IEC 62443 standard, is discussed.

### 4.1.9 Validation

The calculations of the IOP, OOP, IOPP, and OOPP are validated by making a comparison between semi-analytical simulation results and analytic results. The obtained results show that both simulation and analytic results match very well with each other. Moreover, an extensive investigation on how each parameter affects the communication reliability is conducted. Thereby, insightful guidelines can be provided to help obtaining the required reliability.

### 4.2 Overview of the Included Papers

Below the abstracts and a brief description of the contributions of the included papers are provided.

In Papers B and C, the IOPs evaluating single wireless links are derived as proper metrics for the CPS. To evaluate the communication reliability in the case of multiple wireless links with and without the presence of jamming attacks, the OOP, the IOPP, and OOPP are defined and derived in Nakagami-$m$ fading channels in Papers B, C, D, E, and F. Then, by using optimization and machine learning tools considering the obtained closed-form expressions of the selected metrics as the objective functions, the proposed communication protocols are tailored to improve communication reliability, even in the presence of jamming attacks. Especially when interference and/or jamming signals are strong, different techniques, e.g., relaying strategies and retransmission are adopted and evaluated. Different scenarios should use different performance metrics, e.g., the OOPP in Paper E and the outage probability for each source node packet and the OOPP in Paper F. Moreover, detecting interference from colocated clusters or jammers can help the legitimate system adapt to adjust settings and strategies to enhance communication reliability as presented in Paper G. Finally, general guidelines related to power allocation, user pairing, relayer’s position, mobile AP’s position, and relaying protocols are discussed.
The mapping of research contributions to included papers is shown in Table 4.2.

Table 4.2. Mapping of research contributions to included papers.

<table>
<thead>
<tr>
<th></th>
<th>P_A</th>
<th>P_B</th>
<th>P_C</th>
<th>P_D</th>
<th>P_E</th>
<th>P_F</th>
<th>P_G</th>
</tr>
</thead>
<tbody>
<tr>
<td>C_1</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C_2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C_3</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C_4</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C_5</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C_6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>C_7</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C_8</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

4.2.1 Personal Contributions

I have been the main author and driver of the work for all included papers. The co-authors have been involved through brainstorming, discussions, and writing. Furthermore, they have provided feedback on drafts of the papers.

4.2.2 Included Papers

Paper A: Reliability and Fairness for UAV Communication Based on Non-Orthogonal Multiple Access

Authors:
Van-Lan Dao, Hung Tran, Svetlana Girs, Elisabeth Uhlemann.

Summary:
Recently, communication using unmanned aerial vehicles (UAVs) as relay nodes has been considered beneficial for a number of applications. Moreover, non-orthogonal multiple access (NOMA) with users being assigned different signal power levels while sharing the same time-frequency domain has been found effective to enhance spectrum utilization and provide predictable access to the channel. Thus, in this paper we consider an UAV communication system
with NOMA and propose a solution to find the optimal values for the user’s power allocation coefficients (PACs) needed to achieve the required levels of communication reliability. We present a closed-form expression for the PAC of each user and also propose an algorithm for finding the optimal altitude of the UAV required to satisfy the fairness condition for all users. Finally, we provide numerical examples and compare the results for three types of communication environments [68].

Addressing Contribution:
C7.

Author’s Contributions:
The author was the primary driver of the paper, took part in idea generation, determined the performance metrics, implemented the idea, analyzed the results, and wrote most of the text. The other authors helped in writing and provided their feedback and carried out the role of supervisors.

Status:
Published at IEEE International Conference on Communications Workshops, Shanghai, China, 2019.

Paper B: Outage Performance of Pairwise NOMA Allowing a Dynamic Decoding Order and Optimal Pairs of Power Levels

Authors:
Van-Lan Dao, Le-Nam Hoang, Svetlana Girs, Elisabeth Uhlemann

Summary:
In this paper, we evaluate the overall outage probability (OOP) of pairwise Non-orthogonal Multiple Access (NOMA) for both uplink and downlink. We also propose a dynamic decoding order (DDO) together with a fixed pairwise power allocation (FPPA) scheme, in which the optimal decoding order is decided based on the instantaneous channel gains, and thereafter, a pair of power levels is assigned in accordance with the selected decoding order. Exact closed-form expressions of the OOPs for both uplink and downlink pairwise NOMA considering all proposed decoding orders over Nakagami-$m$ fading are derived. Further, we find the optimal fixed power levels for different power allocation strategies so that the OOPs are minimized. Moreover, we investigate the influence of the distances between the source nodes and the access point (AP), the target transfer
rates and the path-loss exponents on the OOPs for all cases of decoding orders. In addition, we benchmark our proposed DDO against other decoding orders in terms of the OOP. The results show that assigning optimal fixed power levels which takes the instantaneous decoding order into account not only improves the communication reliability, but also reduces the complexity and computational load at the AP [50].

**Addressing Contribution:**
C1, C2, C3, C4, and C7.

**Author’s Contributions:**
The author was the primary driver of the paper, took part in idea generation, implemented the idea, carried out performance evaluation, and wrote most of the text. The other authors contributed to performance metrics determination, results analysis, feedback on writing, and carried out the role of supervisors.

**Status:**
Published at IEEE Open Journal of the Communications Society, 2020.

**Paper C: Defeating Jamming Using Outage Performance Aware Joint Power Allocation and Access Point Placement in Uplink Pairwise NOMA**

**Authors:**
Van-Lan Dao, Le-Nam Hoang, Svetlana Girs, Elisabeth Uhlemann

**Summary:**
In this paper, an uplink pairwise Non-Orthogonal Multiple Access (NOMA) scenario using a mobile access point (AP) or an unmanned aerial vehicle in the presence of a jamming attack is considered. To mitigate the influence of the jamming attack, a joint power allocation and AP placement design is proposed. Accordingly, closed-form expressions of the overall outage probability (OOP) and the individual outage probability (IOP) considering imperfect channel state information for each of the source nodes the AP serves, are derived over Nakagami-\(m\) fading channels using dynamic decoding order and fixed pairwise power allocation. We conduct an investigation of the effect of different parameters such as power allocation, source node placements, AP placement, target rates, and jammer location on the OOP and the IOP performance. By adapting the power allocation and the AP placement to the jamming attack, the communication reliability can be increased significantly compared to neglecting
the presence of the jammer or treating the jammer as noise. Since the malicious jammer and the AP have conflicting interests in terms of communication reliability, we formulate a non-cooperative game for the two players considering their positions and the power allocation of the NOMA nodes as their strategies and the OOP as utility function. We propose using hybrid simulated annealing - greedy algorithms to address the joint power allocation and AP placement problem for the cases of both a fixed and a mobile jammer. Finally, the Nash equilibrium points are obtained and then the UAV goes directly to this position and keeps staying there to save power consumption [51].

Addressing Contribution:
C1, C2, C3, C5, C7, and C8.

Author’s Contributions:
The author was the primary driver of the paper, took part in idea generation, implemented the idea, carried out performance evaluation, and wrote most of the text. The other authors contributed to performance metrics determination, results analysis, and feedback on writing, and carried out the role of supervisors.

Status:
Published at IEEE Open Journal of the Communications Society, 2021.

Paper D: Outage Performance Comparison of Adaptive Relaying Schemes Subject to Jamming

Authors:
Van-Lan Dao, Svetlana Girs, Elisabeth Uhlemann

Summary:
Proper relay selection (RS) plays a key role for improving the reliability of wireless networks, especially in the presence of jamming attacks and/or interferers. In this work, we consider various RS schemes based on different criteria, e.g., channel gains and signal-to-interference plus noise ratio (SINR) in different hops, to select the best relayer and then evaluate them using outage probability (OP). We also suggest an RS scheme selecting relayers to maximize the communication reliability in terms of minimizing the OP. The RS strategy takes the effect of jamming attacks and/or interferers into account on both, relayers and the destination. Accordingly, an intensive investigation of the OP of all RS schemes considering also jammers’ positions in various scenarios is
conducted. The results suggest that a combination of RS schemes using channel gains and SINRs of all hops, respectively, achieves the best communication reliability in different scenarios of interference and channel estimation errors. Finally, discussions about the obtained results and the complexity of all RS schemes are presented before providing guidelines on which schemes should be used in different scenarios to improve the communication reliability [69].

**Addressing Contribution:**

C2, C4, C6, and C8.

**Author’s Contributions:**

The author was the primary driver of the paper, took part in idea generation, implemented the idea, carried out performance evaluation, and wrote most of the text. The other authors contributed to performance metrics determination, results analysis, and feedback on writing, and carried out the role of supervisors.

**Status:**

Submitted to IEEE International Conference on Emerging Technologies and Factory Automation, 2023 (accepted).

**Paper E: Defeating Jamming Attacks in Downlink Pairwise NOMA Using Relaying**

**Authors:**

Van-Lan Dao, Svetlana Girs, Elisabeth Uhlemann

**Summary:**

This study explores an incremental relaying strategy in downlink pairwise Non-Orthogonal Multiple Access (NOMA), which involves multiple pairs of nodes near and far from the downlink destinations. The strategy aims to select a near destination node to relay the packet of a far destination node, considering the presence of jamming attacks. To this end, we first derive closed-form expressions for the individual outage probability (IOP) for both near and far destinations in Nakagami-\(m\) fading channels. Next, the overall IOP (OIOP) performance is defined as the maximum value among the obtained IOPs, ensuring fairness among the nodes. To optimize the system, simulated annealing algorithms are proposed to determine the best power allocation and the best relay-destination pairing. We can conclude that both the power allocation and the position/selection of the near destination node significantly impact the OIOP
for a specific pair. However, in the case of multiple pairs of destinations, a
good power allocation alone suffices for each pair, and fixed or even random
destination pairing is satisfactory in the considered context [67].

**Addressing Contribution:**
- C2, C3, C4, C5, C6, and C8.

**Author’s Contributions:**
The author was the primary driver of the paper, took part in idea generation,
implemented the idea, carried out performance evaluation, and wrote most of
the text. The other authors contributed to performance metrics determination,
results analysis, and feedback on writing, and carried out the role of supervisors.

**Status:**
- Submitted to IEEE International Symposium on Personal, Indoor and Mobile
Radio Communications, 2023 (accepted).

**Paper F: Dealing with Jamming Attacks in Uplink Pairwise NOMA Using
Outage Analysis, Smart Relaying and Redundant Transmissions**

**Authors:**
- Van-Lan Dao, Svetlana Girs, Elisabeth Uhlemann

**Summary:**
Outage analysis is an efficient tool for establishing communication reliability
for both individual nodes and the overall wireless network. Closed-form expres-
sions of outage probabilities can be adopted by deep reinforcement learning
(RL) algorithms to optimize wireless networks online. This study focuses on an
uplink pairwise Non-Orthogonal Multiple Access (NOMA) scenario with and
without the support of a relayer, while subject to jamming attacks. We consider
two different relaying protocols, one where the sources and the destination are
within range of each other and one where they are not. The relay node can
be mobile, e.g., a mobile base station, an unmanned aerial vehicle (UAV) or a
stationary node that is chosen as a result of a relay selection procedure. We also
benchmark with a NOMA retransmission protocol and an Orthogonal Multiple
Access (OMA) scheme without a relayer. We analyze, adjust and compare
the four protocols for different settings. Accordingly, we first derive closed-
form expressions for the individual outage probability (IOP) of each source
node link and the relayer link using both pairwise NOMA and OMA. Next, we
analyze the IOP for one packet (IOPP) for each source node considering all possible links between the source node to the destination, taking both phases into account for the considered protocols when operating in Nakagami-$m$ fading channels. The overall outage probability for all packets (OOPP) is defined as the maximum IOPP obtained among the source nodes. This metric is useful to optimize the whole wireless network, e.g., to ensure fairness among the source nodes. Then, we propose a method using deep RL where the OOPP is used as a reward function in order to adapt to the dynamic environment associated with jamming attacks. Finally, we discuss valuable guidelines for enhancing the communication reliability of the legitimate system.

**Addressing Contribution:**
C2, C3, C4, C5, C6, and C8.

**Author’s Contributions:**
The author was the primary driver of the paper, took part in idea generation, implemented the idea, carried out performance evaluation, and wrote most of the text. The other authors contributed to performance metrics determination, results analysis, feedback on writing, and carried out the role of supervisors.

**Status:**

**Paper G: Anomaly Attack Detection in Wireless Networks Using DCNN**

**Authors:**
Van-Lan Dao, Björn Leander

**Summary:**
In this paper, typical use cases are analyzed to highlight the rogue device detection problem. A method for rogue device detection using raw IQ signal data is presented, using deep convolutional neural network (DCNN). An algorithm is proposed for finding optimal number of convolutional layers and their number of filters is provided for the designed DCNN under a constraint of accuracy threshold to decrease the prediction time. The performed simulations indicate that the selected parameters significantly affect the prediction time when using a standard CPU, as compared to a GPU. Moreover, the effects of wireless channel models on the accuracy and prediction time of the designed DCNN model are investigated. Finally, we discuss system-wide reactions of the legitimate system.
when rogue devices are detected, using the IEC 62443 standard. As future work, we envision implementing and evaluating the rogue device detection algorithm in a realistic system, along with system-wide reactions, to investigate its feasibility. Evaluations of different heuristics to decrease the training time are another possible avenue of future work [70].

**Addressing Contribution:**

C8.

**Author’s Contributions:**

The author was the primary driver of the paper, took part in idea generation, implemented the idea, carried out performance evaluation, and wrote most of the text. The other authors contributed to performance results analysis and feedback on writing.

**Status:**

Published at IEEE World Forum on Internet of Things, 2022.
In this thesis, the main goal is to increase and/or provide sufficient performance of wireless networks when used for CPS applications in confined areas. First, suitable performance metrics in terms of outage probability for both single and multiple wireless links are presented. Then, a set of tools in terms of closed-form expressions for the IOP, OOP, IOPP, and OOPP are provided to evaluate the performance of a single wireless link in the system as well as the overall system performance considering all possible links between a source node and its destination. Using these tools, the performance of communication protocols for CPS applications used in confined areas, given certain settings and parameters, can be evaluated both with and without the presence of jamming. As an example, it is shown that pairwise NOMA can be tailored to the requirements of CPS and then used on top of an existing TDMA scheme to enhance reliability without increasing the delay. Various tools are used in different scenarios to select proper settings improving communication reliability for the legitimate system such as the OOP in downlink NOMA relaying and the OOPP in uplink NOMA relaying. A method using machine learning for detecting anomaly nodes in terms of interferers and/or jammers is introduced. Moreover, a method adopting deep RL to deal with a dynamic environment related to jammers is presented. Finally, insightful guidelines on power allocations, decoding orders, node placements, user pairing, etc. are provided, both with and without the presence of an attacker.
5.1 Future Work

In this thesis work, only interference from a jammer and/or any other interferer is taken into consideration. In order to continue improving the communication reliability for the legitimate system, dealing with a cooperative attack between an eavesdropper and jammer should be addressed in the future. Moreover, an evaluation for multi-hop scenarios also needs to be investigated rather than being constrained to two hops protocols as was the case in this thesis.
Bibliography


[51] Van-Lan Dao, Le-Nam Hoang, Svetlana Girs, and Elisabeth Uhlemann. Defeating jamming using outage performance aware joint power allocation


[68] Van-Lan Dao, Hung Tran, Svetlana Girs, and Elisabeth Uhlemann. Reliability and fairness for UAV communication based on non-orthogonal
multiple access. In *IEEE International Conference on Communications Workshops*, pages 1–6, Shanghai, China, 2019.
