Security at the Physical and MAC Layers in Wireless Networks

Dissertation
for the award of the degree
"Doctor rerum naturalium" (Dr.rer.nat.)
of the Georg-August-Universität Göttingen

within the doctoral program Computer Science (PCS)
of the Georg-August University School of Science (GAUSS)

submitted by

Youssef El Hajj Shehadeh

from Chehim (Lebanon)

Göttingen, 2013

Thesis Committee

Prof. Dr. Dieter Hogrefe
Institut für Informatik, Georg-August-Universität Göttingen

Prof. Dr. Xiaoming Fu
Institut für Informatik, Georg-August-Universität Göttingen

Prof. Dr. Kifah Tout
Faculty of Computer Science, Lebanese University of Beirut

Members of the Examination Board

Reviewer: Prof. Dr. Dieter Hogrefe
Institut für Informatik, Georg-August-Universität Göttingen

Second Reviewer Prof. Dr. Kifah Tout
Faculty of Computer Science, Lebanese University of Beirut

Further members of the Examination Board:

Prof. Dr. Xiaoming Fu
Institut für Informatik, Georg-August-Universität Göttingen

Prof. Dr. Jens Grabowski
Institut für Informatik, Georg-August-Universität Göttingen

Jun.-Prof. Dr. Konrad Rieck
Institut für Informatik, Georg-August-Universität Göttingen

Prof. Dr. Stephan Waack
Institut für Informatik, Georg-August-Universität Göttingen

Date of the oral examination: 12. April 2013

Acknowledgments

I would like first to express my deepest gratitude and sincere appreciation to my supervisor and advisor Prof. Dr. Dieter Hogrefe. His supervision, advice, guidance, personal help and friendliness have been key factors that have lead to the successful completion of this thesis. Second, I would like to thank gratefully Prof. Dr. Kifah Tout for his help, advice and for revealing this opportunity to pursue my PhD at the *University of Göttingen*. Without him, none of this would have been true. Also, I am very grateful to my second supervisor Prof. Dr. Xiaoming Fu, for all his time, professional advices and guidance.

My gratitude goes also to the other members of the examination committee: Prof. Dr. Stephan Waack, Prof. Dr. Jens Grabowski, and JProf. Dr. Konrad Rieck. I would like to thank additionally JProf. Dr. Rieck for his useful comments and suggestions during the Post-graduate seminar and Mensa times.

My deepest thanks to all the members of the Telematics group for their help, kindness and support. I am very thankful to Carmen Scherbaum and Udo Burghardt for their help and kindness. Also, I thank gratefully Betty Mayeku, Wissam El Dah and Layal Al Ait for proof-reading my thesis.

Moreover, I am very grateful to the German Academic Exchange Service (DAAD) for the financial support. Great appreciation goes to the contact persons, Ms. Cornelia Hanzlik-Rudolph, and Ms. Anke Bahrani.

Last but not least, I would like to thank my family, brothers and friends for their love and outstanding support throughout the whole period of my PhD. My eternal gratitude goes to my family for their education, support and encouragement in all matters of life.

Abstract: The main objective of this dissertation is to investigate security solutions and issues at the lower layers in wireless networks.

In the first part, the potential of the physical layer in providing security solutions is investigated. Recently, it has been found that the multipath wireless channel in TDD wireless communications can provide a common reciprocal source of randomness that can be leveraged in secret key generation and agreement. Based on this property, many key generation mechanisms have been proposed. In contrary to the common direct quantization and extraction mechanisms, we propose two intelligent mechanisms for secret bits extraction. They are based on mitigating error through optimized guard intervals (GI mechanism) or through phase-shifting the channel taps (PS mechanism). The high efficiency of these two mechanisms compared to the regular quantization mechanisms is manifested through simulations based on a realistic channel model.

We also investigate some practical issues that affect the performance of key generation at the physical layer based on the multipath wireless channel. Delay and Mobility are mainly investigated. In fact, mobility leads to a varying channel. Thus, delay between the channel estimation procedures at the two communicating wireless nodes results into varied channel estimates, hence key disagreement. To tackle these two issues, we propose the Enhanced 3-Way PS mechanism. Through simulation results, this mechanism has been proven to be robust to delay and mobility while still achieving a high secret bit extraction rate. Finally, key reconciliation and error correction are also discussed.

The second part of this dissertation is concerned with securing medium access in wireless networks. In fact, the broadcast nature of wireless communications poses a problem with channel access. A selfish node can get easily a higher share of the common wireless channel by simply manipulating through the medium access protocol parameters, mainly the random backoff selection procedure.

To tackle this problem, we first propose the Random Backoff Control (RBC) mechanism. It is based on controlling the backoff selection procedure to ensure a fair distribution of channel resources and enable simple misbehavior detection. The effectiveness of this mechanism in thwarting misbehavior, compared to other related mechanisms, is manifested through simulations based on the OMNeT++ network simulator.

Last but not least, we investigate scheduling-based medium access schemes and we develop the Self-Organized Distributed Channel Access (SODCA) scheme. Intuitively, a scheduling scheme would be resilient to misbehavior and would achieve a higher bandwidth efficiency than contention-based mechanisms. Distinctively from other proposed schemes, SODCA does not incur any additional overhead and is a distributed, efficient, compatible, misbehavior resilient, and a dynamic scheduling scheme. Through simulation results based on the OMNeT++ network simulator, we demonstrate the high efficiency of SODCA compared to contention based mechanisms in both static and dynamic scenarios.

Contents

Chapter 1

Introduction

Contents

1.1 Background

Wireless communications have undergone considerable improvements and have integrated into human life through various applications. The simplicity, mobility support and fast installation speed of wireless networks have all lead to their rapidly growing popularity. Everyday, we see the growing interest in wireless communications in various applications, ranging from wireless local area networks, Ad hoc networks, sensor networks to connecting every digital device in what we call now the internet of things.

Yet, the open broadcast nature of wireless communications poses many problems, mainly related to security and access control. Indeed, securing communications has always been a major challenge faced by researchers and network engineers in developing standards, protocols and products. Attacks targeting the Internet, private networks and wireless communications have increased enormously over the last decade while the skill and knowledge required to implement them have declined.

The wide spread of digital communications and its acceptance by users have been always threatened by the secrecy of the data transmitted and the privacy of the senders. With the adoption of wireless communications in the everyday-life, users now have become more concerned about the security of their digital communications and their privacy than ever. Users and organizations require different security services that guarantee the security and privacy of their communication. They require guarantees on the integrity, authenticity, and confidentiality of their transmitted data. Furthermore, continuous availability and access control are also very essential features.

Many security standards and protocols have been developed to secure digital communications and provide all required security services. These have been developed, modified and adapted to wireless communications. Traditional security protocols rely mainly on cryptography, hashing functions, and other mathematical properties to fulfill their goals [1]. Yet, nowadays with the widespread of wireless communication and its various applications, these protocols are still far from being the adequate and perfect solutions. Therefore, research on new ways to secure wireless communications is continuously being carried on.

One of the main requirements of communication security is the distribution of secret keys between communicating nodes. Some traditional solutions consider Public Key mechanisms for key exchange [1] requiring a Public Key Infrastructure (PKI) and a Certification Authority (CA). However, PKI mechanisms are only computationally secure and require high computational power. This makes these solutions particularly not appealing in sensor networks, where energy and computational power are limited resources. In addition, the necessity of a CA makes these solutions unpractical in some scenarios, mainly in Ad hoc networks. Other solutions consider key predistribution schemes (see for example [2]). However, key predistribution schemes lack scalability which makes such solutions not very appropriate for large-scale deployment. Besides, key predistribution schemes assume basically fixed and static topologies. Thus, they restrict mobility and are not suitable in dynamic networks.

Recently, there have been a lot of effort invested in seeking other methods of key agreement in wireless networks. This has been motivated by the parallel advances and findings in optical networks. Quantum cryptography [3] has been largely investigated for the purpose of key agreement in optical communications. Indeed, it has been found that the uncertainty principle in quantum physics can be leveraged in key agreement and in securing optical communications. As for wireless communications, the wireless multipath channel has appeared recently as an interesting candidate. Interestingly, it has been found that the multipath phenomenon in wireless communications provides a sort of randomness and diversity that can be leveraged in extracting secret keys (See for example [4, 5, 6, 7, 8, 9]). In fact, many real world measurements have shown that in Time Division Duplex (TDD) wireless communications, the multipath channel forms a reciprocal source of information common for any two communicating nodes, such that other nodes separated by distances greater than the order of a wavelength observe different multipath channels. This is mainly due to the fact that in rich scattering environments, channel gains and phases vary rapidly in space. In other words, this means that an eavesdropper located few centimeters away from both communicating nodes (call them Alice and Bob) observes uncorrelated channel coefficients. Thus, Alice and Bob can leverage their common secret reciprocal channel gains as a common source of randomness to generate a shared-key to secure their communication. Therefore, there is a real potential in the physical layer to secure wireless communications. The question that remains is how to leverage this property in a smart, efficient, and reliable way to achieve a high key extraction rate. The first part of this dissertation is mainly concerned with this question.

On the other hand, the broadcast nature of wireless communications poses many problems related to access control and distribution of resources. In fact, the wireless medium is a common limited resource in wireless networks. Hence, the access to this medium needs to be coordinated in a secure and controlled way. IEEE 802.11 [10] is the *de facto* standard for Wireless Local Area Networks (WLANs). It specifies both the Medium Access Control (MAC) layer and the Physical layer of WLANs. The basic medium access control scheme defined is the Distributed Coordination Function (DCF)[1]. It is a distributed contention resolution scheme and uses the *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) mechanism.

Many security protocols such as WEP, WPA, and WPA2 provide authentication schemes to control the accessibility to the provided services in the network. Yet, these protocols do not provide adequate means to maintain a fair access to the wireless medium and a fair distribution of resources on the different users. The proposed medium access technique in IEEE 802.11 assumes a cooperative behavior of all participating hosts to obtain a reasonably fair throughput distribution. Hence, it is very vulnerable to manipulating and cheating selfish nodes. A malicious node that does not adhere to the medium access scheme can easily obtain an unfair share of the common wireless channel or disrupt the normal operation of the network. Indeed, it has been found that the presence of malicious nodes that deviate from the DCF contention resolution scheme can reduce dramatically the throughput share received by the well behaving nodes [11, 12, 13]. Furthermore, the impact of MAC layer misbehavior can reach the level of a Denial-of-Service (DoS) attack. Therefore, the development of secure medium access schemes, or mechanisms for detecting misbehavior and ensuring a fair channel access is very essential in WLANs. The second part of this dissertation is concerned with this objective.

[1] The IEEE 802.11 standard proposes another access method called Point Coordination Function (PCF). However, this mode is optional and very few APs actually implement it. Moreover, the 802.11e amendment proposed the Enhanced Distributed Channel Access (EDCA) which is an enhancement to DCF that supports Quality-of-Service (QoS) by dividing the different QoS traffic into different access classes with different contention parameters. A similar contention mechanism is used between traffic of same class, mainly traffic with no QoS requirements. Hence, the analysis and results in this dissertation can be easily extended to EDCA. Therefore, we base our analysis on DCF as being the fundamental channel access technique in wireless IEEE 802.11 networks.

1.2 Contributions

This dissertation tackles security issues and solutions on the physical layer and the MAC layer in wireless networks. It is divided into two parts:

1.2.1 Key Generation on the Physical Layer

In the first part of this dissertation, we investigate key generation on the physical layer in wireless networks based on the multipath wireless channel. Recently, several key generation and agreement mechanisms have been proposed. They are mainly based on 3 steps: a direct quantization of channel coefficients, reconciliation by public discussion, and finally privacy amplification. Direct quantization of random coefficients results in a considerable number of discrepancies between the derived secret bits at the two nodes. For that reason, a reconciliation stage is required to remove these discrepancies and obtain a lower probability of error. This is generally accomplished through a public discussion phase, where some data as syndromes and parity bits are exchanged, followed by an error correction phase to correct any occurring errors. However, public discussion implies loss of secrecy. Consequently, privacy amplification is applied to increase the entropy of the obtained bits at the cost of a lower efficiency. As a matter of fact, there is a reliability-efficiency tradeoff in this case.

In this dissertation, we develop intelligent mechanisms of key generation from multipath wireless channels. The main goal of an intelligent mechanism is to achieve a lower probability of error even before the reconciliation stage. We target smart quantization and public discussion mechanisms that lead to a high bit extraction rate without involving any loss of secrecy. Our first contribution is our proposed **Guard-Intervals** (GI) quantization method that is based on separating the quantization regions by guard bands, optimized to achieve a high efficiency at a lower probability of error. Our second contribution is our novel **Phase Shifting** (PS) method. It is based on a public discussion step that involves the exchange of phase shifts to decrease significantly the error probability *without loosing any secrecy.* Both analytical and simulation results approve the efficiency of this method in achieving a high secret bit extraction rate at a low probability of error even before the reconciliation stage.

In a later section, we tackle practical issues that affect the performance of key generation based on the multipath wireless channel. Delay between channel estimates and mobility are mainly investigated. In fact, mobility leads to a varying channel. Hence, a delay in the channel estimation at the two communicating nodes leads to different channel estimates and hence key discrepancies. Therefore, robustness to delay and mobility is an essential requirement of a reliable secret key generation mechanism based on the wireless multipath channel. Our third contribution targets achieving this feature through our proposed **Enhanced 3-way PS** method. This method is then proven to be *robust* to delay and mobility while still achieving a high key generation rate.

Furthermore, we investigate other ways to increase the key generation rate. And finally, we discuss the application of error correcting codes to further increase the reliability of the extracted keys.

1.2.2 Advanced and Secure Medium Access Schemes

In the second part of this dissertation, we investigate security issues on the MAC layer of wireless networks. We highlight the negative impact of misbehavior in medium access on the total network throughput and the distribution of resources. To tackle this problem, many solutions have been proposed following basically two trends. Some approaches have considered developing misbehavior detection mechanisms based on the DCF contention mechanism. Whereas other approaches have targeted developing advanced and secure medium access schemes. Indeed, DCF is not only vulnerable to misbehavior but also suffers from a high collision rate which leads to a suboptimal use of bandwidth. This drawback of contention-based schemes has lead to a growing interest in scheduling schemes. Intuitively, a scheduling scheme would result in a low collision or collision-free transmission, and would allow simple misbehavior detection by monitoring any out-of-schedule transmissions.

Following the first trend, our first contribution is the proposed **Random Backoff Control** (RBC) mechanism. RBC is based on minor modifications to the DCF backoff mechanism to thwart misbehavior and hence ensure a fairer access to the channel. The misbehavior resilience of RBC is manifested through simulations in the presence of aggressive selfish nodes.

Afterwards, we consider the design and development of an advanced and secure medium access scheme that is resilient to misbehavior and more efficient than contention-based schemes. Therefore, we investigate scheduling-based channel access schemes. So far, there have been many efforts to establish scheduling-based channel access schemes. The IEEE 802.11 standard includes the Pointed Coordinated Function (PCF) mode. In this mode, the AP is given the task of scheduling transmission between the nodes. However, centralized schemes are definitely not suitable for wireless networks when there is no perfect information about the network dynamics and the traffic rates at the different wireless nodes. Thus, efforts were more focused on establishing a distributed scheduling scheme. Many distributed scheduling schemes have been proposed. Yet, none has really been adopted for many reasons. Some incur a large overhead, while others target only establishing a static schedule and are not suitable for dynamic networks. Finally, misbehavior resilience was not considered thoroughly in these schemes.

Our second and most significant contribution in this area is the development of a novel scheduling-based medium access scheme, called **Self-Organized Distributed**

Channel Access (SODCA). It is based on establishing a schedule between the different backlogged nodes in a network in a distributed self-organized way without necessitating any exchange of traffic information. As far as we know, it is the first scheduling-based medium access scheme that achieves all our design goals of being distributed, dynamic, efficient, compatible, misbehavior resilient and finally it incurs no additional overhead over the currently used medium access schemes. We manifest the efficiency of this scheme through extensive simulations using the OMNeT++ network simulator. In addition to its misbehavior resilience, the SODCA scheme achieves up to 20% higher network throughput than the DCF scheme without modifying the communication protocol or the format of any of the control and data packets.

1.2.3 Publications

The contributions in this dissertation have been published/ pending to be published in the following international journals and conferences:

- Y. El Hajj Shehadeh, M. Hotait, K. Tout, and D. Hogrefe, "SODCA: A Distributed Dynamic Scheduling Channel Access Scheme for Wireless Networks," *to be submitted (Conference Paper).*

- Y. El Hajj Shehadeh, M. Hotait, K. Tout, and D. Hogrefe, "Random Backoff Control to Thwart Malicious Behavior in WLANs," *in Proceedings of the 19th IEEE International Workshop on Local and Metropolitan Area Networks*, Brussels, Belgium, April 2013.

- Y. El Hajj Shehadeh, O. Alfandi and D. Hogrefe, "Towards Robust Key Extraction from Multipath Wireless Channels," *Journal of Communications and Networks- Special Issue on Physical-layer Security*, Vol. 14, No. 4, pp. 385-395, August 2012.

- Y. El Hajj Shehadeh, O. Alfandi and D. Hogrefe, "On Improving the Robustness of Physical-layer Key Extraction Mechanisms against Delay and Mobility," *in Proceedings of the 8th International Wireless Communications and Mobile Computing Conference*, Limassol, Cyprus, August 2012.

- Y. El Hajj Shehadeh, A. El Falou, and D. Hogrefe, "On Enhancing the Reliability of Key Extraction Mechanisms from Wireless Channels," extended abstract, *Workshop on Physically-augmented Security for Wireless Networks (PILATES 2012)*, Kaiserslautern, Germany, March 2012.

- Y. El Hajj Shehadeh, O. Alfandi, K. Tout, and D. Hogrefe, "Intelligent Mechanisms for Key Generation from Multipath Wireless Channels," *in Proceedings* *of the 10th IEEE Wireless Telecommunications Symposium (WTS 2011)*, New York, USA, April 2011.

- Y. El Hajj Shehadeh, and D. Hogrefe, "An Optimal Guard-Intervals Based Mechanism for Key Generation from Multipath Wireless Channels," *in Proceedings of the 4th IEEE International Conference on New Technologies, Mobility and Security (NTMS 11)*, Paris, France, February 2011.

1.3 Organization

This dissertation is organized as follows:

Chapter 2 provides an overview of the different security services required in a digital communication system. It also reviews briefly some of the main mechanisms usually implemented to provide these services.

Chapter 3 gives an overview of wireless propagation and the multipath wireless channel. First, a brief review of the different phenomena affecting a wireless signal is given. Multipath, spatial diversity, and channel reciprocity are mainly discussed as they characterize the wireless channel as a common reciprocal secret source of information that can be leveraged to derive a secret key between two communicating wireless nodes. After that, we review channel modeling and describe the channel model used in our simulations.

Chapter 4 investigates secret key generation on the physical layer of wireless communications. We first review some related work and give a short information-theoretic background on key extraction from common randomness, reconciliation, and privacy amplification. After a description of the system model, we present our proposed key generation mechanisms and the simulation results that show the effectiveness of our proposed methods. Afterwards, we tackle some practical issues that affect the performance of secret key generation from wireless channels. Delay between channel estimates and mobility are mainly investigated. Then, an enhancement to the key generation mechanisms is proposed to ensure robustness against delay and mobility. Finally, reconciliation and key verification are discussed.

Chapter 5 tackles the problem of misbehavior on the MAC layer in wireless networks. We first review the basic medium access scheme used in IEEE 802.11 networks and highlight its vulnerability to misbehavior in addition to its bandwidth efficiency. We mainly focus on backoff misbehavior which allows a selfish node to get an unfair share of the wireless channel. We review some of the related work on this topic and propose the Random Backoff Control (RBC) mechanism. This mechanism provides a countermeasure against MAC layer DoS attacks and ensures a fairer distribution of network resources. The second part of this chapter is concerned with the design of an advanced and secure medium access scheme. A review of some of the related work on this topic is first given. Afterwards, we describe our proposed Self-Organized Distributed Channel Access (SODCA) scheme. Distinctively from all proposed solutions, our novel medium access scheme is a distributed, efficient, secure and dynamic scheduling scheme. Nevertheless, it does not incur any additional overhead. The efficiency of SODCA is manifested through extensive simulations based on the OMNeT++ network simulator.

Chapter 2

Security Basics

Contents

Securing communications has always been a big challenge faced by researchers and network engineers in developing standards, protocols and products. Attacks targeting the Internet, private networks and wireless communications have increased enormously over time while the skill and knowledge required to implement them have declined.

The wide spread of digital communications and its acceptance by users have been always threatened by the secrecy of the data transmitted and the privacy of the senders. Users have now become more concerned about the security of their digital communications and their privacy than ever. Users and organizations require different security services that guarantee the security and privacy of their communication. Secrecy of their data is one of the biggest requirements. Moreover, they require guarantees on the integrity and authenticity of their transmitted messages. Finally, continuous availability of the network is also an important required feature.

In this chapter, we investigate these different security requirements and the main mechanisms used. First, we discuss the different types of attacks that may threaten the security and privacy of users. After that, we discuss the different security services; and finally we review some of the basic mechanisms that are being used to satisfy the different security and privacy requirements.

2.1 Security Attacks

2.1.1 Passive Attacks

A Passive attack targets eavesdropping on or monitoring data transmissions without tampering the transmitted messages. This type of attack is by its nature difficult to detect since the attacker listens only to the communication without any intervention. It is even more facilitated in wireless communication due to its broadcast nature. Therefore, security measures should be taken into account to prevent any adversary from accessing or reading the contents of the transmitted information.

2.1.2 Active Attacks

Active attacks have in general a bigger impact on the security and the privacy of communications. They are related to any act of modifying, tampering, eliminating or even creating messages.

An attacker may tamper or modify the transmitted messages so that they contain false information or become undecodable. He can also disrupt communications and eliminate transmitted messages. This may lead to a delay or disorder in the transmitted messages which might produce an unauthorized effect. Such modifications of messages may also lead the legitimate nodes to perform unauthorized actions or get compromised by the attacker and abused to perform larger scale attacks. Moreover, by modifying the contents of messages, an attacker can deplete the resources of a legitimate node.

Another form of active attacks is the masquerade attack, where an attacker pretends to be a different entity. By impersonating this entity, it might be able to have some privileges or access to more resources. For example, in a replay attack, an attacker captures passively messages transmitted by legitimate nodes and transmits them to appear as a legitimate node and get access to some network resources. Therefore, it is necessary to provide strong authentication of the identity of a node.

In addition, an attacker can inject false messages into the network that may lead to the disruption of communication (a Denial of Service attack (DoS)) or may mislead the legitimate nodes into performing other actions that may exhaust their resources (power, bandwidth). It may also target a specific entity by dropping all messages directed toward a specific destination, thus depriving it of network services.

Moreover, an attacker might not respect the communication protocols and leverage some vulnerabilities to get an unfair share of the network resources. This is mainly called the misbehaving attack. For example, in wireless communications, an attacker might not respect the medium access protocol to get a bigger share of the wireless channel. In fact, the Medium Access Control (MAC) layer does not provide any secure distribution of resources and is based on cooperative behavior of participating nodes. It assumes that these nodes follow the contention mechanism to get access to the channel. However, an attacker or a selfish node might not follow this contention procedure and get a full or an unfair access to the channel.

In conclusion, active attacks have different characteristics than passive attacks. Although passive attacks are difficult to detect, security measures could be implemented to prevent them. On the other hand, it is difficult to prevent active attacks completely, due to their wide variety. However, security measures could be implemented to diminish their impact or to detect them and apply appropriate reaction mechanisms.

2.2 Security Services

A security service is defined as a service provided by a protocol layer to ensure adequate security of the communicating system. Security services implement security policies and are implemented by security mechanisms [14]. There are many security services provided by the different network layers. In this section, we describe these different services before discussing some security mechanisms in the next section.

2.2.1 Authentication

Authentication is a critical security service in wireless communications. It is concerned with assuring that the communication is authentic. When receiving a message for example, it is very important to ensure that the message is indeed from the source it claims to be from.

Moreover, authentication is very essential when logging onto a network. In this case, it is important to authenticate the logging user in order to ensure that this user has privileges to access the network. There are mainly three basic schemes used for authentication:

- *Something you know*: This is the most commonly employed scheme. It is typically a password, a code or a key sequence that proves that the user is who he claims to be and that he is authorized to access the network. However, this scheme is not very secure and is easy to compromise. Despite that, it is the most widely used scheme.

- *Something you have*: This authentication mechanism is based on something you own as a key, a badge, a token card, or some device that provides you with access. The drawback of this mechanism is that the owned "thing" could be stolen or lost.

- *Something you are*: This relies upon some physical or behavioral characteristics that are specific to a certain entity. Biometrics, for example, can be used to authenticate one's identity based on finger, iris or voice prints. In wireless communications, there have been recently a lot of works on using some physical layer characteristics for authentication, as clock skews, hardware fingerprints or even the radio channel.

Very often, security protocols apply one or a combination of more than one of these schemes to provide a secure authentication scheme. However, some of these schemes may not be available in some networks and scenarios.

2.2.2 Access Control

Access control comes directly after authentication and is closely related to it. It is also referred to as authorization and it refers to the ability to control what resources the user has access to or which privileges he has. In other words, access control is the determination of the level of authorization of an entity.

2.2.3 Data Confidentiality

Confidentiality is related to the secrecy of the data and the privacy of the users. It signifies the protection of transmitted data against passive attacks by protecting the transmitted information from unauthorized disclosure. This is usually achieved by encrypting the information so that it is not meaningful to unauthorized entities. Confidentiality is also concerned with the protection of the traffic flow from analysis. This requires a protection of the privacy of the users so that an attacker should not be able to detect the source, destination or even any other characteristic of the traffic flow that might jeopardize the privacy of the communicating entities.

2.2.4 Data Integrity

Data integrity is achieved by preventing unauthorized or accidental improper changes to the data transmitted. Hence, the data integrity service refers to the ability to protect information transmitted from unauthorized, uncontrolled or even accidental alterations and modifications. It targets at ensuring that the messages have been received as sent with no duplication, insertion, modification, reordering or replays.

2.2.5 Nonrepudiation

Nonrepudiation is concerned with providing a proof that a certain message has been transmitted (or received) by an entity. It refers to the ability to prevent the transmitter (receiver) from denying the transmission (reception) of a certain message, data or file. Thus, when a message is sent, the receiver can prove that the transmitter has actually sent the message even if he denies. On the other hand, when a message is received, the sender can prove that the alleged receiver did receive the message. This capability is crucial in some areas, for example in e-commerce or in wireless networks where sensitive data is exchanged.

2.2.6 Availability and Secure Distribution of Resources

Availability refers to the requirement of any communication system to be reliable and resilient to different types of attacks. It aims at ensuring that the system resources are available and accessible upon demand by an authorized entity [14]. In other words, this service addresses the security concerns raised by denial of service attacks.

A secure distribution of network resources is also a required property of a communication system and is directly related to availability. It aims at ensuring equal share of resources between the different users. Fairness is mainly important in wireless communications where the wireless medium is shared between the different users. Thus, a security measure should be implemented to ensure a fair share of resources. The requirement for this service is mainly raised on the level of the MAC layer in wireless communication systems. Actually, in the current implemented protocols, fairness is not guaranteed and is only based on the cooperation of the participating nodes.

2.3 Security Mechanisms

As we have discussed briefly above, security mechanisms should be provided to maintain data confidentiality, data integrity, authentication, and nonrepudiation. The more effective these mechanisms are toward achieving these goals, the more secure is the communication system.

Basically, data confidentiality is achieved by cryptographic processes where a message is encrypted through a key so that it is unintelligible to anyone not in possession of the key. Hence, a confidential secure communication between two entities can be obtained through encryption and decryption using cryptographic keys. In some cases, the encryption and decryption keys are the same. This corresponds to *symmetric key* *encryption*. While in other cases, the encryption and decryption keys are different which corresponds to *asymmetric key encryption*.

On the other hand, authentication, nonrepudiation, and integrity can be obtained through proper hashing and message digest functions. A trusted certification authority is then required to provide entities with digital certificates.

In this section, we describe briefly some of the common security mechanisms. We first investigate cryptography and highlight the differences between symmetric key encryption and asymmetric key encryption. After that, we give an overview on public key systems. Basically, we describe the Diffie-Hellman key exchange, message authentication and integrity mechanisms, and digital signatures. Moreover, we describe briefly digital certificates and the public key infrastructure.

2.3.1 Cryptography

2.3.1.1 Symmetric Key Encryption

Symmetric key encryption is the first idea that comes in mind when you think about encryption. It corresponds to the encryption and decryption of a message using the same key, normally called secret or shared key. Hence, both parties use a shared key and a common encryption algorithm to exchange encrypted messages. Consequently, any party not in possession of the shared key cannot decrypt the messages. Fig. 2.1 illustrates the concept of symmetric key encryption.

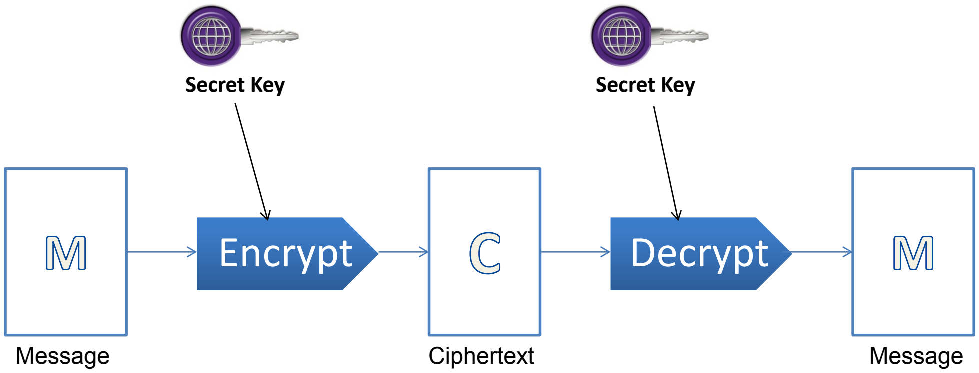


Figure 2.1: Concept of symmetric key encryption.

Symmetric key encryption is characterized by its fast and relatively low computational complexity. However, its main weakness is the requirement of key management and distribution. Indeed, it is not trivial to establish a shared key over an unsecured network without being compromised. Therefore, a secure method to distribute shared keys is required. In section 2.3.2, we describe one of the methods used to agree on a secret key.

Moreover, symmetric key encryption alone does not provide any means for authentication and nonrepudiation. Therefore, its application alone is not sufficient to provide all the security services. Some of the known and widely deployed symmetric key systems include DES, 3DES, AES, Blowfish, RC4.

2.3.1.2 Asymmetric Key Encryption

Asymmetric cryptography was first introduced by Whitfield Diffie and Martin Hellman of Stanford University in 1976. It is also commonly known as public key cryptography. Unlike symmetric key cryptography which is based on one single key, asymmetric cryptography is based on a key pair: a private key and a public key. As their names signify, one key is kept private while the other is made public. Another property of these keys is that knowing one key does not reveal the other, so that revealing the public key does not endanger the security of the system.

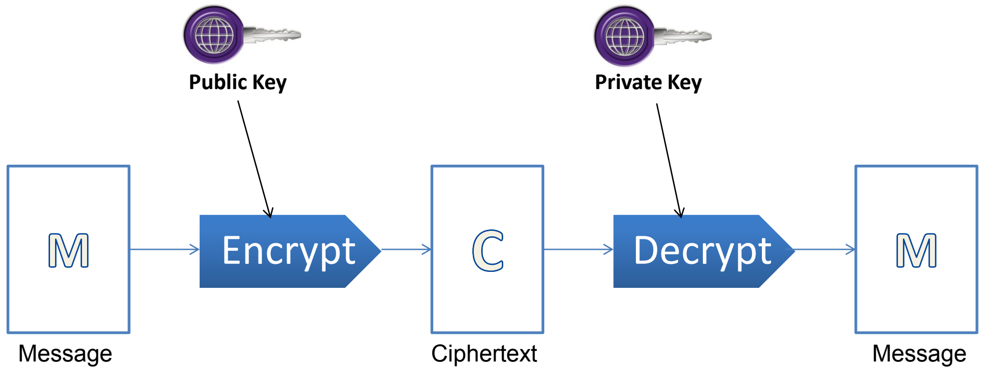


Figure 2.2: Concept of asymmetric key encryption.

In Fig. 2.2, we illustrate the asymmetric key encryption procedure. First of all, public keys are exchanged between the two parties, call them Alice and Bob. A message sent to Alice, for example, is encrypted by the public key of Alice. Hence, Alice can use its private key to decrypt the ciphertext and read the content of the message. On the other hand, all other nodes not in possession of the private key of Alice cannot read the content of the message.

With the aid of asymmetric cryptography, it is possible to establish a secure communication between any two entities in a network. It is only required to exchange the public keys even on an unsecured channel[1] in contrast to symmetric cryptosystems where the shared key should be transmitted securely. Therefore, a public key cryptosystem is more scalable than a symmetric key system as it allows a spontaneous secure communication between any two entities over an insecure network.

However, asymmetric key encryption is known to be more computationally expensive than symmetric key encryption. We will see in the later sections that it is mainly used as a way of authentication and nonrepudiation and for the purpose of exchanging secret keys.

2.3.2 Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange algorithm was the first public-key algorithm introduced by Diffie and Hellman [15]. The purpose of this algorithm is to allow two users to derive a shared secret key that can be used for subsequent symmetric encryption of the messages.

The algorithm's security depends on the difficulty of computing discrete algorithms. Hence, it is a computationally secure key exchange algorithm. Briefly, this algorithm can be explained in the following way. Each of the two communicating entities generates a pair of public-private keys. Then they exchange their public keys. And finally, each applies his private key to the other's public key to calculate a shared secret key. More information about this algorithm can be found in [1, 14, 16].

However, it is important to note here that an authentication mechanism is required to authenticate the exchanged public keys.

2.3.3 Hashing and Message Authentication

Hashing is a mechanism that can be deployed to ensure data integrity. A hash function takes as input a message of variable size and outputs a fixed-length hash value called a message digest which forms a cryptographic checksum of the message.

Before sending the message to Bob, Alice computes a message digest which is appended to the original message and sent to Bob. Bob then removes the hash value from the received message and runs by himself the same hash operation to compute the hash value. Data integrity can be verified by comparing the two hash values. If the message has been modified in any way during transit, the hash values will not match. And in case the hash values match, Bob can assure that the message has not been modified and consequently data integrity has not been compromised.

[1] However, this exchange is vulnerable to man-in-the-middle attacks. Therefore it should be accompanied with an authentication mechanism to ensure the identity-public key binding.

Although hashing and message digests provide data integrity, message authenticity is still not guaranteed. However, this can be provided when the message is hashed with the secret key shared between the two parties, i.e. the sent hash value now depends on the used key.

Hash functions are required to be one way only. This means that there should be no way (or it is computationally difficult) to reverse the hash value and obtain the message content. Moreover, effective hashing requires that the possibility of collision is very limited. A collision occurs when two or more unique messages have the same hash value. Thus, it is important that different messages have different hash values.

2.3.4 Digital Signatures

Hashing and message authentication codes provide data integrity and authenticity. However, they do not provide nonrepudiation. This is provided through digital signatures which helps in protecting the two parties not only from a third party but also from each other.

A digital signature allows a receiver to authenticate the identity of the sender, verify the integrity of the message and prove to any other party that the sender did send the message. Digital signatures use a combination of hashing and asymmetric encryption in order to secure the hash value exchanged between the two parties. In other words, a digital signature is an asymmetrically-encrypted form of a message digest.

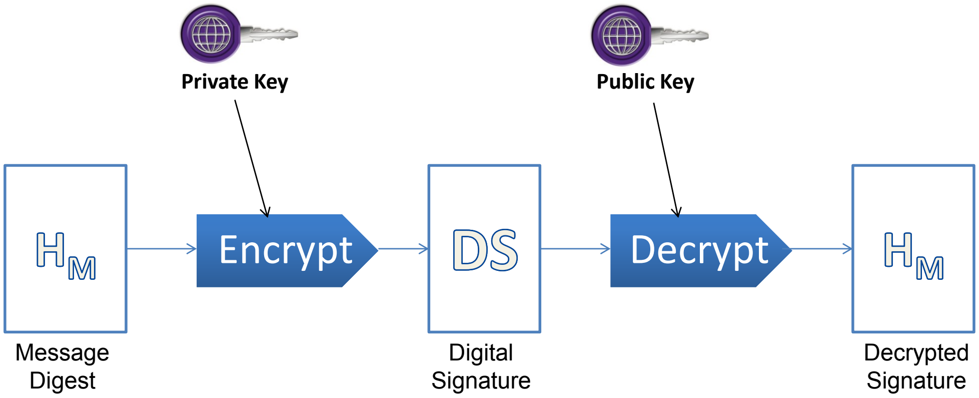


Figure 2.3: A simple digital signature system.

To sign a message, the sender performs a hashing on the cleartext message obtaining a message digest. After that, the message digest is encrypted using the private key (Fig. 2.3). The receiver decrypts the digital signature using the public key of the sender and verifies the hash value. Consequently, the receiver can verify if the source is authentic, since the public key would not decrypt a message digest value that has been encrypted using a different private key. Therefore, we can say that digital signatures ensure data integrity, authenticity and provide means for nonrepudiation as we will see in the next sections.

Apart from that, we note that digital signatures follow a different procedure as compared to asymmetric encryption. In asymmetric encryption, the public key is used for encryption and the private key is used for decryption. This ensures that only the entity owning the private key can decrypt the ciphertext. On the other hand, the reverse operation is performed when calculating a digital signature. In this case, the private key is used for encryption and the public key is used for decryption. This ensures that any entity in possession of the sender's public key can verify the digital signature.

2.3.5 Public Key Infrastructure

2.3.5.1 Digital Certificates

Digital signatures can be used to verify the integrity of a message and that it was issued from an entity with the corresponding public key. Yet, it is still not possible to verify if that public key indeed belongs to the individual or entity that claims to own it. Therefore, a binding scheme between identities and public keys is needed.

A digital certificate is a method that enables the binding of an individual or entity to a public key. It is issued by a trusted third party known as a Certificate Authority (CA) according to a Public Key Infrastructure (PKI). The digital certificate is signed by the CA using its private key. Then, any entity can use the CA's widely known public key to verify the authenticity of the digital certificate.

Digital certificates issued by CAs provide an independent means to confirm that an individual or entity is in fact who he claims to be. Hence, digital certificates provide a means for a secure first-time spontaneous communication. In fact, a digital certificate guarantees the receiver with a high level of confidence that the digital signature indeed belongs to the sender.

Considering again the example of Alice and Bob, Alice can now send Bob the digital certificate signed by a known CA. This enables Bob to verify the identity of Alice and verify that the key used by Alice is in fact hers. As a result, any digitally signed message by Alice can now be authenticated. In addition, this allows nonrepudiation. Indeed, Bob can now prove that the message he obtained was sent by Alice whose public key is certified by a certificate authority.

Table 2.1 shows some of the possible contents of a digital certificate. Basically, a digital certificate includes the identity of the individual or entity, his public key, a

Digital Certificate
Name: Individual, organization, entity
Owner's public key
Certificate expiration date
Certificate's serial number
Name of issuing CA
Issuing CA's digital signature

Table 2.1: An example of a digital certificate structure

certificate expiration date, a serial number, the name of the issuing CA and finally the CA's digital signature to verify the authenticity of the digital certificate. It could also include other information depending on the type of the certificate.

It is worthwhile to mention here that digital signatures accompanied with digital certificates have a greater legal authority than handwritten signatures. In fact, digital signatures are very hard to forge. Hence, a digital signature provides a proof that the digitally signed document has not been altered and that it has been issued by the sender who is in possession of the private key used to sign the document.

2.3.5.2 Certificate Authorities

As mentioned previously, a certificate authority is a private or public entity that plays the role of a trusted third party. A CA issues digital certificates that authenticate the identity of those to whom the certificates are issued. These certificates are signed by the private key of the CA. Hence, the CA's public key must be trustworthy and widely known to have a reliable and effective public key system. Actually, trustworthiness is an important requirement of a CA, since a CA will be relied on to verify the bindings between identities and public keys.

2.3.5.3 Public Key Infrastructure

A PKI is a hierarchy of CAs where a root CA certifies subordinate CAs. Also, each higher level CA can be used to authenticate lower level CAs, thus preserving the hierarchy.

2.4 Summary and Discussion

In this chapter, we have presented the different security services that are required towards achieving a secure, trustworthy and privacy-preserving communication system. After that, we have briefly reviewed some of the security mechanisms used to provide these security services. We have discussed cryptography, both symmetric and asymmetric, in addition to key exchange, authentication, and non-repudiation mechanisms.

To obtain a complete solution, we have seen that a public key infrastructure is required. Indeed, even for key exchange, a trusted third party is needed to authenticate the identity of the other party. This makes these solutions not very appropriate in some applications where a trusted third party is not available, or access to this party is not continuously and reliably possible.

Moreover, these solutions are computationally expensive. Basically, the public key mechanisms, including the Diffie-Hellman key exchange mechanism, require a relatively high computational power. Hence, these solutions are not suitable for some low cost wireless devices which have a very low computational power and run on batteries. Take for example sensor devices. These devices are characterized by their low cost and a very low computational power which is not sufficient to perform complex computations. In addition, continuous complex computations can deplete their energy resources.

For these reasons, many researchers have been investigating possible alternatives. In this dissertation, we investigate the potential of the physical layer in joining the security game. Actually, almost no credit has been given to the physical layer in the currently implemented security solutions. We investigate the generation of shared secret keys on the physical layer level and discuss physical layer continuous authentication.

Chapter 3

Overview of the Multipath Wireless Channel

Contents

The wireless channel has many particularities that need to be considered to achieve a reliable wireless communication. Indeed, wireless communication is mainly characterized by its broadcast nature, in addition to the different phenomena affecting a propagating radio signal. Yet, some properties of the wireless channel can be leveraged to provide some functions, like multiple antennas, or for security purposes as we will see throughout this dissertation. In this chapter, we give an overview of the multipath wireless channel. We first discuss the different phenomena that affect wireless propagation, i.e. reflection, refraction, shadowing, path loss, etc... And we show how these lead to what we call the multipath phenomenon which characterizes the wireless propagation. Afterwards, we discuss channel reciprocity and how this property provides a transmitter-receiver pair with a source of randomness. Finally, we review channel modeling for simulation purposes. We consider the generic Rayleigh channel model and more specific ones like cluster-based models. Then, we present the TGn channel models [17] which were proposed by the IEEE 802.11 Task Group n as channel models for simulation purposes, particularly for wireless communications following the IEEE 802.11 standards.

3.1 Radio Propagation

A radio signal is mainly characterized by its broadcast nature. It can propagate through different mediums with different dielectric properties, or get reflected by different obstacles until reaching finally its destination. The former gives rise to the phenomenon of **Refraction** where the radio wave changes its direction and speed when crossing two mediums of different dielectric properties. Whereas the latter gives rise to the phenomenon of **Reflection**, where a part of the radio wave is reflected when hitting an obstacle. In this case, the reflection coefficient (percentage of the reflected power from the received power of the radio wave) is dependent on the size of the obstacle in addition to its dielectric properties. In addition, radio propagation is also affected by **Diffraction** and **Scattering**.

Furthermore, the power of the wireless signal decreases as the signal travels through the space. Indeed, **path loss** is caused by the dissipation of the power transmitted by the transmitter in all directions. As a result, the received power is expected to be a function of the traveled distance. However, there are many other factors affecting the radio signal. The presence of obstacles and reflecting, refracting, scattering and absorbing objects lead to variations of the received power even at the same distance from the transmitter. This phenomenon is called **Shadowing**.

Path loss and shadowing together govern the average power of the radio signal received at the receptor. For this reason, they are mainly referred to as *large-scale fading*[1]. On the other hand, the combination of the different radio signals traversing different paths, called **Multipath** phenomenon, leads to *small-scale fading* where the power of the received signal varies dramatically over relatively small distances.

To be able to model the wireless channel, it is essential to estimate accurately the effect of these phenomena on the radio propagation. This can be solved using Maxwell's equations with appropriate boundary conditions. However, the complexity of these equations makes them impractical as a general modeling tool to model the wireless channel. Therefore, we normally use simplified techniques to model the wireless channel as we will see in the later sections. These models consist mainly of estimating the wavefronts as simple particles and using simple geometric equations.

In the following section, we introduce path loss and shadowing which give rise to *large-scale fading*. Then, we discuss the multipath phenomenon which is a main particularity of wireless propagation.

[1] Shadowing is also sometimes separated from path loss and is called *medium-scale fading*

3.1.1 Path Loss

3.1.1.1 Free-space Path Loss

Free-space path loss designates the loss in the power of the radio signal as it traverses through the *free space*, i.e. assuming there are no obstacles between the transmitter and the receiver. It is an important factor as it determines the maximum range of wireless communication. The free-space path loss, for a radio wave of wavelength λ, can be expressed as [18]:

$$P_{L_{FS},dB} = -10log(\frac{G_l \lambda^2}{(4\pi d)^2}), \tag{3.1}$$

where d is the traversed distance by the radio wave, and $\sqrt{G_l}$ is the product of the transmit and receive antenna radiation patterns in the LOS (Line-Of-Sight) direction.

As a result, we observe that the power of the receive signal decreases proportionally to the square of the traveled distance in case of free-space communication. We will see in the following sections that the received power decreases even more rapidly in other propagation scenarios.

3.1.1.2 2-Ray Model

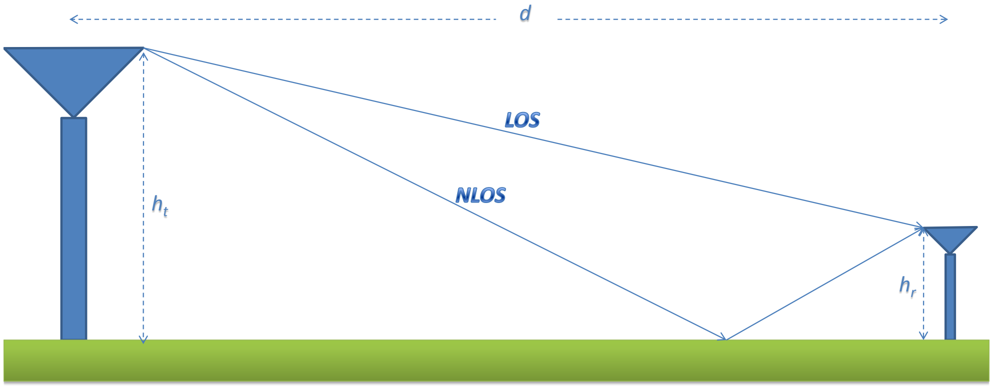


Figure 3.1: 2-Ray model consisting of a direct LOS ray and a reflected NLOS ray.

The 2-ray model is mainly used to model a communication where there is only one single ground reflection (see Fig. 3.1). An example of this situation would be over water communication (between two ships). The received signal is then the combination of the LOS component and the reflected component or ray. These two rays combine constructively or destructively depending on the phase difference. For distances greater

Environment	α range
Urban macrocells	3.7-6.5
Urban microcells	2.7-3.5
Office Building (same floor)	1.6-3.5
Office Building (multiple floors)	2-6
Store	1.8-2.2
Factory	1.6-3.3
Home	3

Table 3.1: Some typical Path Loss exponents [18]

than a certain distance called **critical distance** d_c, they start to combine destructively. In this case, the path loss (for $d > d_c$) can be found to be [18]:

$$P_{L_R,\,dB} = -10log(\frac{G_l h_t^2 h_r^2}{d^4}), \tag{3.2}$$

where h_t and h_r are respectively the transmitter's and receiver's antenna heights.

We observe, in this case, that the power of the received signal drops more rapidly as a function of the traveled distance. It is now inversely proportional to d^4.

3.1.1.3 Empirical Path Loss Models

In general, the wireless environment is more complex and cannot be modeled by free-space path-loss or ray tracing methods. However, a number of path loss models have been elaborated for typical wireless environments such as urban, rural or even indoor environments. These models were elaborated based on statistical measurements. An example of these models are the Okumura and Hata models [18]. However, for reasons of brevity, we will not go into the details of these models. We just summarize these approaches by the simplified path loss model which estimates the path loss to be inversely proportional to d^α:

$$P_L = \frac{K}{d^\alpha}, \tag{3.3}$$

where K is a constant and α varies depending on the environment. Some typical values of α for different environments are given in Table 3.1.

3.1.2 Shadowing

Empirical path loss models, discussed above, provide an estimation of the mean attenuation as a function of the distance from the transmitter. However, there are other factors that affect the power of the received signal. Indeed, the radio signal can be blocked or attenuated by different obstacles. The resulting impact varies according to the relative position of the receiver even at the same distance from the transmitter. In addition to that, changes in reflecting surfaces and scattering objects result in variations of the received power at a given distance. Consequently, these variations lead to a random attenuation, called **Shadowing**. Empirical channel measurements have shown that this random attenuation can be modeled through a log-normal distribution. Thus, the total attenuation would be the sum of the path loss attenuation (in function of the distance) and a random variable following the log-normal distribution given by:

$$p(\psi_{dB}) = \frac{1}{\sqrt{2\pi}\sigma_{\psi_{dB}}} exp\left[-\frac{(\psi - \mu_{\psi_{dB}})^2}{2\sigma^2_{\psi_{dB}}}\right], \ \psi > 0, \tag{3.4}$$

where $\mu_{\psi_{dB}}$ and $\sigma_{\psi_{dB}}$ are respectively the corresponding mean and standard deviation in dB.

3.1.3 Multipath and Spatial Diversity

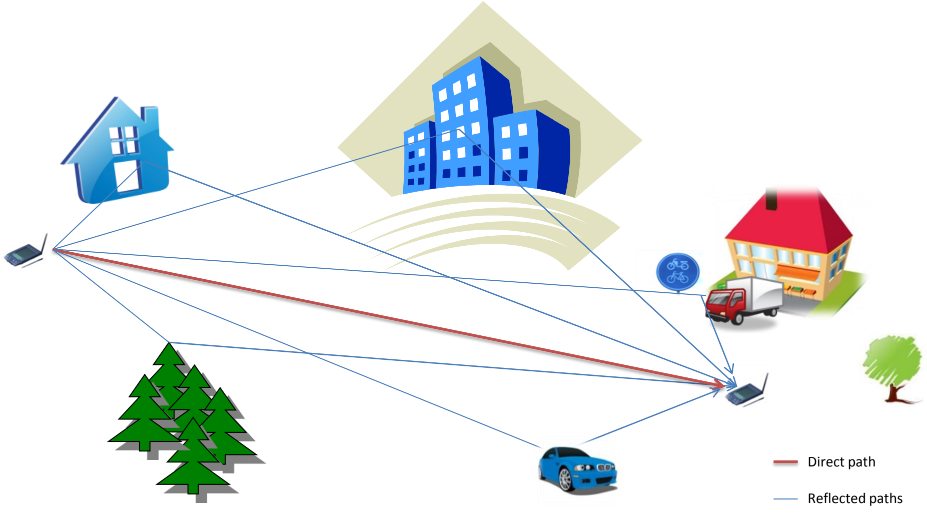


Figure 3.2: Multipath in wireless channels

Due to the broadcast nature of wireless communications, a transmitted signal may traverse different paths before arriving at the destination. It might be subject to different phenomena such as reflection, refraction, and scattering. Therefore, it undergoes different attenuations and phase shifts as it traverses the different paths. As a result, the received signal would be the combination of signals arriving through different paths with different attenuations, delays and phase shifts. This phenomenon, called **Multipath**, manifests itself through dramatic rapid changes in the signals amplitude and phase. It leads to what is called *fast fading* or *small-scale fading*. In fact, multipath characterizes wireless channels by a sort of spatial diversity such that antennas separated by small distances experience uncorrelated wireless channels.

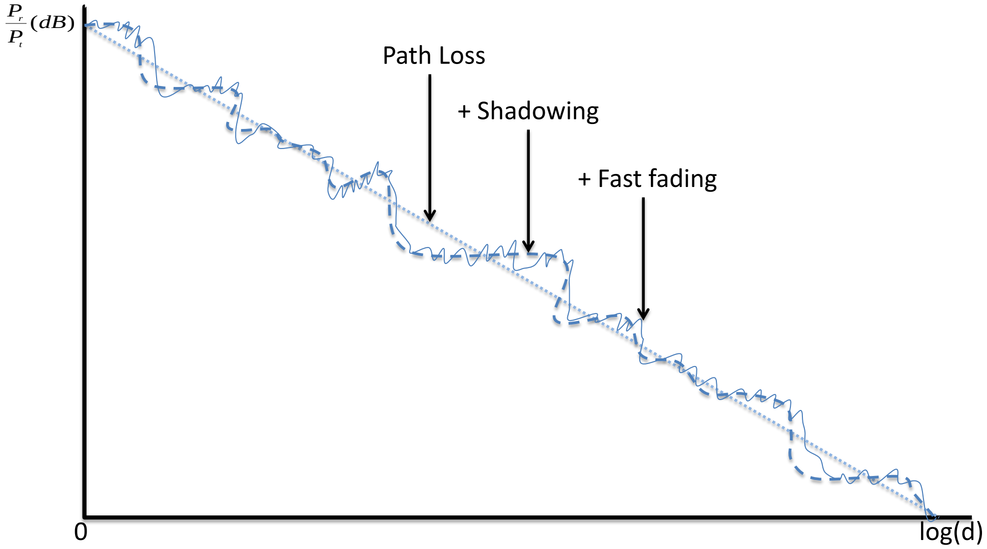


Figure 3.3: Combined path-loss, shadowing, and fast-fading

In Fig. 3.3, we show the combined result of path loss, shadowing and fast fading on the received power as a function of the distance. Path loss manifests itself through a linear decrease of the received power as a function of $log(d)$, shadowing leads to medium-scale fading, while multipath leads to dramatic rapid changes in the signal strength.

3.2 Channel Reciprocity

Reciprocity in point-to-point radio communications is guaranteed by the physical laws of electromagnetics [19]. The electromagnetic reciprocity theorem was first discovered by Lorentz in 1896 [20, 21]. This theorem has many applications in antenna theory. Mainly, it is used to establish the fundamental relation between the transmitting and receiving patterns of an antenna radiating into a *linear* and *isotropic* medium. Assume for example that two antennas A1 and A2 are separated from each other where in the first case A1 is transmitting while A2 is receiving; and in the second case, A2 is transmitting while A1 is receiving. And considering the two antennas as a two-port network, it can be shown that the mutual impedances between these two ports are identical.

This means that in radio communications, the roles of the transmitting antenna and the receiving antenna can be interchanged while the radio transfer characteristics remain the same. In other words, the electromagnetic propagation from Alice to Bob follows same paths and undergoes same effects as that from Bob to Alice. Therefore, when two antennas with linear components radiate identical signals in an isotropic and linear medium, the signals received at the two antennas will be identical.

The channel impulse response is normally used to represent a wireless channel. It is defined as the signal received at an antenna by an impulse transmitted at the other antenna. This measurement incorporates the different phenomena affecting radio communications such as reflection, refraction, diffraction and finally multipath. In fact, radio communication is characterized by its broadcast nature such that a transmitted signal travels freely in all directions, gets reflected, refracted or diffused before reaching its destination. Hence, the channel impulse response incorporates the different paths traveled by the signal and the different attenuations and phase shifts. This phenomenon called multipath results in an output signal that differs significantly as the locations of the transceivers are changed.

In conclusion, the reciprocity theorem provides a wireless transmitter-receiver pair with a common source of randomness which is the experienced multipath wireless channel. In Chapter 4, we investigate leveraging this source of common information in cryptography, mainly in deriving shared secret keys.

3.3 Channel Modeling

3.3.1 Rayleigh Channel

Analysis of multipath and practical measurements have shown that the wireless channel impulse response can be approximated as a Rayleigh channel (having a Rayleigh distribution). As a result, the channel impulse response, in base band at time instant t, to a delta pulse which stimulated the channel at time τ can be expressed as:

$$h(t,\tau) = \sum_{l=0}^{L-1} h_l(t)\delta(\tau - \tau_l), \tag{3.5}$$

where δ is the unit impulse function, L is the length of the channel (number of taps), while $h_l(t)$ and τ_l represent the complex gain and delay of the $(l+1)^{th}$ channel tap at time instant t.

Interestingly, it has been found that $h_l(t)$ follows circular complex Gaussian distributions in case of non line of sight. In this case, the signal envelope follows a Rayleigh distribution. Whereas in the case of line of sight, it follows a Rician distribution.[2]

Many statistical models have been proposed and elaborated to model the channel impulse response. The main challenge of these models was to encompass the different phenomena that affect the radio signal as in realistic environments, in addition to the time-variation due to mobility. In the following section, we present two simplified approaches: the discrete-time approach and the space-time cluster-based approach.

3.3.1.1 Discrete-Time Model

One of the most common discrete-time models that are widely used to represent realistic fading channels is the improved discrete Jake's model [22, 23]. It is a deterministic model for simulating time-correlated Rayleigh fading waveforms and it is used to describe a mobile channel as presented in Eq. 3.6. The Jake's fading Model helps in estimating the variation of the Rayleigh channel in time accordingly with the Doppler shift. Particularly, for each channel tap, the model assumes that M equal-strength rays arrive at the moving receiver with uniformly distributed arrival angles α_n, such that the ray n experiences a Doppler shift $\omega_n = \omega.cos\alpha_n$, where $\omega = (2\pi f v)/c$ is the maximum Doppler phase shift, v is the node speed, f is the carrier frequency, c is the speed of light, and $\alpha_n = 2\pi n/M$:

$$h_l(t) = \sigma_l \cdot \sum_{n=1}^{M} e^{j(\omega_n t + \varphi_n)}, \tag{3.6}$$

In this equation, φ_n is a random variable uniformly distributed over $[0, 2\pi]$ and σ_l^2 is the average power of the $(l+1)^{th}$ channel tap.

3.3.1.2 Time Correlation

In a wireless communication system, the mobility of the nodes or reflecting objects leads to a time variation of the channel. Therefore, it is important to calculate the time-spaced autocorrelation function as it determines the channel correlation as a function of time-shift Δt. For example, if a channel estimate is acquired at time t, the autocorrelation function determines the correlation between this estimate, and the channel at some time $t + \Delta t$ in the future. The coherence time is defined as the time period over which the channel remains highly correlated (with a correlation coefficient of 0.9 or 0.7 commonly used). The normalized autocorrelation function of a Rayleigh fading

[2] In this dissertation, we focus mainly, without loss of generality, on NLOS components since LOS components, when existing, can be simply subtracted from the channel impulse response.

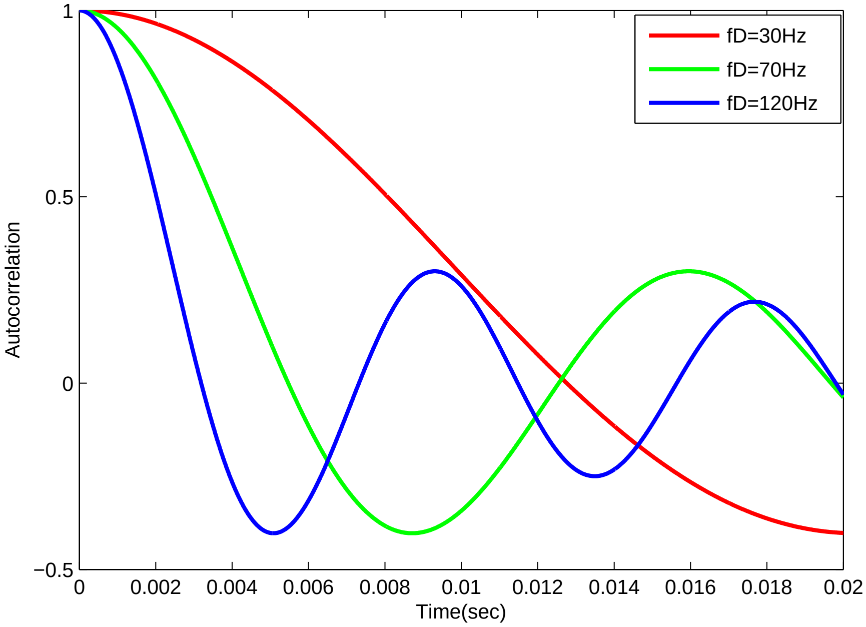


Figure 3.4: Autocorrelation function as a function of time for different Doppler frequencies.

channel with motion at a constant velocity is a zeroth-order Bessel function of the first kind:

$$R(\Delta t) = J_0(2\pi f_D \Delta t), \tag{3.7}$$

where $f_D = fv/c$ is the maximum Doppler frequency.

In Fig. 3.4, we trace the autocorrelation function as a function of time for different maximum Doppler frequencies. We observe that the autocorrelation gets zero after a certain time which corresponds actually to an antenna spacing of 0.4λ. Another observable effect is that the signal re-correlates then with itself. However, the main reason for this is the error in approximating the autocorrelation function as a Bessel function. Real world measurements have shown that the channel remains decorrelated for higher distances [24]. This property of wireless channels means that nodes separated by sufficient distances observe decorrelated channels. We will see later in Chapter 4 how this spatial property of wireless communications can be leveraged to derive a shared secret key.

3.3.1.3 Doppler Spread Spectrum

The Doppler power spectral density of a fading channel describes how much spectral broadening the Doppler shift causes. In particular, this shows how a pure frequency, e.g., a pure sinusoid, which is an impulse in the frequency domain is spread out in the frequency domain when it passes through the channel. It is the Fourier transform of the time-autocorrelation function. For Rayleigh fading, it can be written as:

$$S(f) = \begin{cases} \frac{1}{\pi f_D \sqrt{(1-\frac{f}{f_D})^2}}, & |f| < f_D \\ \quad 0 \quad , & |f| > f_D \end{cases} \tag{3.8}$$

3.3.2 Cluster-based Modeling Approaches

The Rayleigh channel model is a more generic model that fits some scenarios where there is a high density of reflectors. However, it is generally a statistical model. Therefore, it is difficult to study the space-time variation of the channel based on this model.

The cluster-based approach aims at a better study of the spatial and temporal characteristics of the wireless channel. It was mainly developed by Saleh and Valenzuela [25], and further elaborated by Spencer et al. [26], Cramer et al. [27], and Poo and Ho [28]. It involves mainly modeling the channel through a limited number of main reflecting clusters around the receiver. In this case, each cluster will be reflecting different rays coming from different paths with different amplitudes and phases. These would be then arriving at the receiver with a certain Angle Of Arrival (AOA).

Based on this approach, the i_{th} multipath component at the receiver may correspond to a single cluster or to multiple components with similar delays arriving from multiple reflecting clusters. We note that any two components with delays τ_1 and τ_2 are said to be nonresolvable if their delay difference does not exceed the inverse of the signal bandwidth: $|\tau_1 - \tau_2| < |B^{-1}|$. In this case, the amplitude of the summed signal will undergo fast variations due to the constructive and destructive combination of nonresolvable multipath components. On the other hand, when the delay difference is bigger than the inverse of the signal bandwidth, we say that the two components are resolvable and this leads to inter-symbol interference.

3.3.3 TGn Channel Models

The Task Group n defines 6 channel models [17] for simulating different environments ranging from small office environments to large space and outdoor environments:

- Model A with $0ns$ rms delay spread, flat fading model.
- Model B with $15ns$ rms delay spread, 2 clusters.

- Model C with 30ns rms delay spread, 2 clusters.
- Model D with 50ns rms delay spread, 3 clusters.
- Model E with 100ns rms delay spread, 4 clusters.
- Model F with 150ns rms delay spread, 6 clusters.

Moreover, the authors in [17] show a summary of all parameters required for the complete channel characterization. For each channel model, the following parameters are listed:

- Tap Power
- Tap AoA (Angle of Arrival)
- Tap AoD (Angle of Departure)
- Tap AS (Angle Spread) at the receiver
- Tap AS (Angle Spread) at the transmitter

We will not go deep into explaining each of these channel models and their parameters since it is not the purpose of this dissertation. However, we show the parameters of channel model F only in Appendix A, as we tend to use it later in our simulations. We note that model F is defined as to simulate large space indoor or outdoor environments. Therefore, it is characterized by its diversity and large rms (root mean square) delay spread.

3.4 Summary

In this chapter, a short overview of the multipath wireless channel was given. We have revised briefly the main phenomena in radio propagation and we have highlighted the multipath effect as the main particularity of wireless channels. Multipath has been shown to give wireless channels a sort of diversity, such that antennas or nodes separated by short distances, even less than half a wavelength, observe uncorrelated channels: an interesting particularity of wireless channels that can be leveraged in various applications. In the next chapter, we will see how this phenomenon can be used for various purposes, mainly for generating secret keys. In the second part of this chapter, we have reviewed the most common approaches to model wireless channels. And finally, we presented the TGn channel models, particularly the channel model F which will be used in our simulations.

Chapter 4

Secret Key Generation on the Physical Layer

Contents

Wireless communications have undergone considerable improvements and have integrated into human life through various applications, mainly by the widespread of mobile Ad hoc and sensor networks. But due to the broadcast nature of wireless communications, security remains a major concern in many applications. Actually, traditional security protocols rely mainly on cryptography, hashing functions, and other mathematical properties to fulfill their goals [1]. Yet, nowadays with the widespread of wireless communication with its various applications, these protocols are still far from being the adequate and perfect solution.

One of the main requirements of communication security is the distribution of secret keys between communicating nodes. Some traditional solutions consider Public Key Infrastructure (PKI) mechanisms for key exchange [1] in the presence of a Certification Authority (CA). But PKI mechanisms are only computationally secure and require high computational complexity. In addition, the requirement of having a CA makes these solutions unpractical in some scenarios, mainly in Ad hoc and sensor networks. Other solutions consider key predistribution schemes (see for example [2]). However, key predistribution schemes lack scalability which makes such solutions not very appropriate for large-scale sensor deployment or mobility.

Recently, there have been a lot of effort invested in seeking other ways to secure wireless communications. For example, quantum cryptography [3] has been largely investigated for the purpose of key agreement in optical communications. Indeed, it has been found that the uncertainty principle in quantum physics can be leveraged in key agreement and in securing optical communications. As for wireless communications, the wireless multipath channel has appeared recently as an interesting candidate. Interestingly, it has been found that the multipath phenomenon in wireless communications provides a sort of randomness and diversity that can be leveraged in extracting secret keys (See for example [4, 5, 6, 7, 8, 9]). In fact, many real world measurements have shown that in Time Division Duplex (TDD) wireless communications, the multipath channel forms a reciprocal common source of randomness for any two communicating nodes; such that other nodes separated by distances greater than the order of a wavelength observe different multipath channels. This is mainly due to the fact that in rich scattering environments, channel gains and phases vary rapidly in space. In other words, this means that an eavesdropper which is located few centimeters away from both communicating nodes (call them Alice and Bob) will observe uncorrelated channel coefficients (See Chapter 3 for more details). Thus, Alice and Bob can leverage their common secret reciprocal channel gains to generate a suitable shared-key for their communication.

In this chapter, we investigate secret key generation on the physical layer of wireless communications. We start by summarizing some of the related work on this topic. A brief information-theoretic background on key extraction from common randomness, reconciliation, and privacy amplification is given; and we summarize the latest key generation and agreement methods. Then, the system model is described. Afterwards, we present our proposed key generation mechanisms and we demonstrate the effectiveness of these mechanisms through analysis and simulation results. In the following section, we tackle some practical issues that affect the performance of secret key generation from wireless channels. We investigate mainly time delay between channel estimates and mobility. And we propose a modification to our proposed key generation mechanism improving robustness against delay and mobility. Finally, we discuss reconciliation and key verification which form the last steps of a key generation and agreement procedure.

4.1 Related Work

Physical layer security has been an active area of research in the last decade. The idea of generating keys based on the characteristics of the radio channel was first introduced by Hassan et al. in their pioneering work in [29]. Since then, many efforts have been invested in generating secret keys on the physical layer.

Many of these efforts have investigated generating keys using functionalities provided by current of-the-shelf devices. These are mainly based on the quantization of the **RSSI** (Received Signal Strength Indicator) measurements. This parameter is provided by the physical layer based on calculating the average received signal power over a certain period. They also consider a *Reconciliation* stage to enhance the reliability of the extracted key, and finally a *Privacy Amplification* stage to enhance the secrecy. These approaches were validated by practical implementations and measurements using of-the-shelf devices or Universal Software Radio Peripherals (USRP) [30, 31, 32].

On the other hand, some approaches have considered leveraging the whole information provided by the multipath channel. In this case, the whole Channel Impulse Response (CIR) or Channel State Information (CSI), represented by the complex gains of the different channel taps, is considered. In fact, as we have seen earlier, these taps are characterized by being independent and having a uniform phase distribution. As a result, a higher number of secret bits can be extracted by leveraging the whole channel impulse response.

Indeed, channel-phase based quantization methods have three major advantages. First, the uniform distribution of the phases of the channel taps implies a higher level of secrecy [18]. Second, a higher key generation rate can be achieved by leveraging the whole channel impulse response and quantizing the phases of the different channel taps. Third, this allows a spontaneous key extraction, as it is only required to have an estimate of the channel impulse response at a certain instance instead of needing to estimate the average received power over a certain time window. However, RSSI-based approaches have the advantage of being implementable in most of-the-shelf devices, and therefore they do not require significant hardware modifications. In fact, RSSI is usually available to the higher layers in most wireless transceivers. In addition to that, RSSI based schemes are more robust to synchronization issues.

For a theoretical comparison of the key generation rates based on CSI and on RSSI, the reader is advised to read [33]. The authors in this paper derive the secret key capacity in the case of CSI quantization and in the case of RSSI quantization and prove the superiority of the former one.

In this section, we review these two approaches and show a summary of the recent related work on each. But first, we present information theoretic studies in this area. In fact, there have been many more generic approaches investigating generating secret keys from correlated sources of randomness. We also describe *reconciliation* and *privacy amplification*, as these steps are essential in many proposed key extraction and agreement methods. After that, we review the latest approaches of generating secret keys based on RSSI measurements. Then, we discuss the latest CIR-based attempts to generate secret keys. And in the last section, some other proposed methods for generating secret keys on the physical layer are also summarized.

4.1.1 Information-theoretic Perspective

From an information-theoretic point of view, many authors [34, 35, 36] explore the possibility of generating secret keys from correlated sources of randomness.

Maurer in his pioneering work in [34], demonstrates that it suffices for two nodes to be in access to a common source of information, observed differently by other nodes, to achieve perfect cryptographic security regardless of the enemy's computing power. He actually defines the notion of the *secret key rate* and derives upper and lower bounds on the achievable size of the generated key.

Let us consider for example X, Y, and Z as random variables observed by Alice, Bob, and Eve, respectively. X, Y, and Z are characterized by the probability density function P_{XYZ}. Maurer defines the secret key rate of X and Y with respect to Z, denoted by $S(X;Y||Z)$, as the maximum rate at which Alice and Bob can agree on a shared secret key S while keeping the rate at which Eve obtains information arbitrarily small. Hence, the secret key rate of X and Y with respect to Z is upper bounded by:

$$S(X;Y||Z) \leq min[I(X;Y)], I(X;Y|Z)] \tag{4.1}$$

where $I(X;Y|Z)$ designates the mutual information between X and Y given Z.

On the other hand, a nontrivial lower bound on the secret key rate is:

$$S(X;Y||Z) \geq max[I(Y;X) - I(Z;X), I(X;Y) - I(Z;Y)] \tag{4.2}$$

This lower bound shows an interesting aspect of the key rate. It shows that a difference of the mutual information can be exploited to derive a secret key. This means that if Eve has less information about Y than Alice or about X than Bob, then such a difference of information provides a positive key generation rate.

4.1.2 Reconciliation

Due to the reciprocity principle, the same key is expected to be derived. Yet, discrepancies might occur due to the nonsymmetric noise and interference at the two nodes and due to hardware variations. Moreover, the variation of the channel requires a simultaneous estimation of the channel at the two parties. However, this is not practically possible in half duplex communications. Hence, slightly varied channel estimates would be obtained at the two nodes which may lead to some discrepancies in the derived keys. To cope with this problem, some works have considered simple schemes based on probing the channel multiple times and choosing the best RSSI measurement or averaging over several probes. However, this leads to a very low key generation rate especially when long keys are sought. A more reliable solution to this problem is to apply information reconciliation.

Information reconciliation, also referred to as *public feedback* or *error correction*, is the process of detecting and correcting errors by public discussion targeting a higher probability of agreement between the derived keys [37]. It is mainly based on the exchange of syndromes or parity check bits and the application of an error correcting code [38, 39, 40].

However, the error correction procedure is slightly different in this case. In fact, the derived keys (call them K and K') are random vectors which have some discrepancies. Hence, the purpose of the error correction stage is to correct these discrepancies but at the lowest possible secrecy cost since any information exchanged during the public discussion decreases the entropy of the derived key. Many solutions have been proposed to sort out this problem. A direct approach consists of encoding K using a systematic encoder and the transmission of parity check bits (or syndromes). In this case, K is considered as an *Infoword* and is input to the encoder. The obtained parity check bits are then sent to node B which uses its own derived key K' and the received parity check bits, as an input to the decoder which outputs K in case all errors have been successfully corrected.

Another cryptographic primitive called **Secure Sketch** has been also proposed to cope with this problem. It is also based on using an error correcting code. Yet, no parity check bits are transmitted. Instead, a codeword c is chosen randomly from the codebook C of the error correcting code. c is then xored with K to obtain the secure sketch: $SS(K) = s = K \oplus c$ which is transmitted to node B. Node B calculates $c' = K' \oplus s$ and decodes c' to obtain a common secret infoword in case the number of bit differences between K and K' is less than the error correction capability of the error correcting code.

4.1.3 Privacy Amplification

Information reconciliation achieves a higher reliability but at the expense of a loss of secrecy. In fact, the public discussion and transmission of parity check bits during the reconciliation stage leads to a leakage of information. It is immediately apparent that the use of an error correcting code reduces the number of secret bits by a ratio equal to the rate of the code R. In addition to that, other factors might lead to a loss of secrecy. For example, if Eve's channel observations are not perfectly uncorrelated from that of Alice-Bob's, then the derived key is not perfectly secure.

To cope with this problem and to distill perfect secret keys, privacy amplification [41, 42] is necessary. This can be achieved by using universal hash functions [42, 43, 44, 45], or by using extractors [45, 46, 47, 48, 49].

4.1.4 RSSI-based Key Generation

RSSI-based key generation is mainly based on quantizing the RSSI measurements provided by the physical layer to generate common secret bits. In this section, we summarize the recent approaches in this area.

In [4], Mathur et al. have used a two-level crossing excursion-based quantization algorithm to extract bits from **CIR** and **RSSI** measurements. Their algorithm have been evaluated through theoretical and numerical studies providing important insights on the appropriate probing rate and the quantization parameters. They have further validated their proposed algorithm through experiments using an $IEEE$ 802.11 development platform. Two approaches were considered, one based on the channel impulse response and the other based on the received signal strength indicator. In their experiments, the CIR was extracted per-packet basis from the preamble of a format-compliant 802.11a packet which makes their approach equally applicable to off-the-shelf 802.11 hardware. On the other hand, they have used off-the-shelf devices to collect coarse RSSI measurements. In both approaches, they have showed by experiments that it is possible to practically achieve key establishment rates of ≈ 1 bit/sec at an infinitesimally small probability of error in an indoor wireless environment.

This algorithm was further improved in [5, 6, 7]. In [5], an over-quantization method was included followed by a reconciliation stage and finally a privacy amplification stage.

The authors have applied a 1/2 rate LDPC (Low Density Parity Check) code with error correction based on the exchange of log likelihood ratio estimates to achieve an improved secret key generation rate of 10 bits/sec.

Similarly, in [6, 7], Jana et al. have proposed an adaptive scheme to extract multiple bits from a single RSSI measurement. The scheme includes information reconciliation to remove any discrepancies between the extracted bits, and finally applies a privacy amplification mechanism to the reconciled bits to obtain a higher entropy bit stream. The authors have performed extensive real world measurements in different scenarios and settings and they have discussed the effectiveness of RSSI-based secret key extraction. Moreover, in [7], the authors investigate key extraction in MIMO (Multiple Input Multiple Output) systems. They consider a MIMO-like sensor testbed and perform RSSI measurements to extract secret keys. To enhance the performance of their mechanism and decrease the bit mismatch rate especially in MIMO systems, they introduce an iterative distillation step before the information reconciliation stage. It is mainly based on eliminating measurements that are likely to lead to mismatched bits at Alice and Bob.

In [50], Patwari et al. introduced a framework for the extraction of secret bits from a series of radio channel measurements, called HRUBE (High Rate Uncorrelated Bit Extraction). The framework includes 3 main steps: interpolation, transforming for decorrelation, and a multibit adaptive quantization method. The authors argue that it is not practically possible in most transceivers to obtain simultaneous channel measurements due to the half-duplex nature of the wireless communication. Therefore, the authors tend to collect channel samples at some instants and use fractional interpolation filtering to allow nodes to estimate what the measurements would have been if they have been made simultaneously. After that, they propose a Karhunen-Loéve transform (KLT) to convert the obtained channel vectors into uncorrelated components. As for the quantization, the authors propose an adaptive quantization scheme achieving a higher efficiency than the usual censoring scheme. They provide an analysis of the probability of bit disagreement in the generated secret keys and perform an experimental implementation in Crossbow telosB wireless sensor nodes. Their experimental results showed that the implemented HRUBE system can achieve a secret key generation rate of 22 bits/sec at a bit disagreement rate of 2.2 percent, or 10 bits/sec at a bit disagreement rate of 0.54 percent.

Based on the HRUBE framework, a more robust bit extraction method, called ARUBE (Adaptive Ranking-based Uncorrelated Bit Extraction) has been proposed in [51]. It targets reducing the non-reciprocities caused by different hardware characteristics by including a ranking step after the interpolation filtering. Compared to the HRUBE extraction method, this method is more robust to differences in hardware, adapts to the channel environment, can be implemented in wireless motes, and produces, for medium and high SNR channels, $30\% - 60\%$ more bits per sample with a low probability of bit disagreement. Indeed, the tested method has been proven to be able to extract 40 bits/sec at a bit disagreement rate of 0.04 percent.

On the other hand, Azimi-Sadjadi et al. have followed a different approach to quantize the RSSI values [52]. Their approach is mainly based on quantizing the deep fades in the received signal. Consequently, a measurement is encoded as a 0 if it is lower than a deep fade threshold and 1 otherwise. They argue that this method is more robust to non-reciprocities between the channel measurements. Moreover, they have proposed a method to enhance the entropy of the extracted bit stream, called secure fuzzy information reconciliation. It is mainly based on using fuzzy extractors which are characterized by their error correction capability in addition to privacy amplification [53]. However, the reliance on deep fades to extract secret bits results in a relatively low secret key generation rate.

In [54, 55], Wilhelm et al. have validated the correlation of measured RSSI values by performing measurements using MICAz sensor nodes. The authors have developed a key generation mechanism based on RSSI measurements provided by the sensor nodes. They have considered leveraging multiple available channels and applying multi-level quantization to increase the key generation rate. Moreover, to increase the error tolerance, they have considered collecting a number of samples and calculating their average value. They have also applied information reconciliation by using an error correcting code and the transmission of a public reconciliation vector providing information about the distance of the derived key to the nearest codeword. Consequently, privacy amplification was applied by using randomness extractors and universal hash functions.

Using higher bandwidths and multiple channels in the frequency domain to enhance the secret key generation rate has been investigated in [56]. In their paper, Forman et al. consider a 200MHz bandwidth divided into 80 different and independent subchannels. Consequently, they tend to quantize the normalized amplitude and phase of the subcarriers to generate secret keys.

Channel reciprocity was also validated in UWB (Ultra Wide Band) communication systems [57]. In their paper, the authors perform a two level quantization of the received signal strength to generate a secret key.

Apart from that, some works tackle the problem of generating secret keys in stationary channels [58, 59, 60, 61]. In [58], Aono et al. investigate using ESPAR (Electronically Steerable Parasitic Array Radiator) antenna to create artificial fluctuations of the channel characteristics. Their method is mainly based on fluctuating the channel characteristics intentionally using beamforming techniques of the ESPAR antenna. Hence, more randomized and stronger keys can be extracted using this innovative technique thus achieving a higher secret bits extraction rate. Indeed, using their proposed scheme, multiple channel probing packets can be transmitted consecutively even in stationary channels, each with a different random beamform vector used during the transmitting and receiving phase at the access point. Whereas the user terminal is associated with an omni-directional antenna. In addition, the authors target a high probability of key agreement by probing the channel multiple times and then choosing the best RSSI measurements by public discussion and agreement between the two parties. They further enhance the reliability of the key generation mechanism by applying error correction using a BCH error correcting code. Finally, key verification is accomplished by using a one-way hash function. Experiments in different scenarios using $ZigBee^{TM}$ chips were performed to validate the proposed key generation mechanism.

An improvement to this key generation mechanism was proposed in [59]. It is mainly based on including an RSSI interleaving scheme which enables to acquire more randomized and stronger secret keys. The authors have also conducted experiments based on $ZigBee^{TM}$ chips to validate their key generation mechanism. Experimental results showed that a probability of success of 99.998% would be obtained when 128-bit secret keys are exchanged every two seconds. They have also verified the secrecy of the derived keys by applying the FIPS (Federal Information Processing Standard) PUB 140-2 [62] statistical test for random numbers.

This method was further improved in [61] by applying multi-level quantization to increase the key extraction rate. However, these approaches require special antennas which make them non-ubiquitous and expensive solutions.

In addition, many works have considered leveraging multiple antennas to enhance the key generation rate. Actually, Zeng et al. were one of the first to investigate key generation in real multiple-antenna wireless systems [63]. In their paper, they consider quantizing RSSI measurements at multiple antennas and applying multi-level quantization. Both guard intervals based quantization and excursion-based quantization are considered to reduce the probability of error. Their method includes a public discussion phase consisting of agreement on the antennas to be used, the quantization levels, the excursion size, the guard interval, and the RSSI measurements to be quantized. Further, they apply a simple bit-wise xor function as a privacy amplification scheme to increase the entropy of the derived key.

In [60], a new scheme using multiple antennas is proposed where a common private key is generated based on the variation produced by antenna switching. In this scheme, Kituara et al. propose to compare the signal strength at two antennas to generate a secret key instead of using the conventional threshold method.

It is also interesting to study the channel probing rate for the purpose of key generation. In this realm, it is important to consider the pioneering work of Wei et al. in [64] where a relationship between the optimal probing rate and the bit generation rate (BGR) is derived. The authors develop a mathematical model of channel probing and argue that channel probing should not be too fast to achieve a desirable BGR; but only fast enough to avoid using the channel inefficiently. They have proposed a scheme based on Lempel-Ziv complexity to estimate the entropy rate of the channel statistics which governs the BGR and they have used a Proportional-Integral-Derivative (PID) to adjust dynamically the probing rate to achieve the desired BGR.

More recently, Zan et al. have investigated the robustness of key extraction against active attacks [65]. In their paper, they consider the case of a physically-active attacker capable of provoking small fluctuations in the wireless environment. They propose a differential technique to quantize the RSSI measurements and a moving average to remove the effect of small predictable fluctuations and enhance the security of the derived key.

Liu et al., in [66], discuss the reliability of quantization using thresholds and propose a fading trend key generation mechanism based on transforming the trend of the RSSI to bits instead of the usual threshold quantization. In addition, they introduce a relay node assisted scheme for key generation between nodes which are not in the transmission range of each other. However, the security of this scheme relies on the trustworthiness of the relay node.

These approaches emphasize the possibility of generating secret bits from the wireless channel. However, they are still far from what can be achieved due to the hardware limitations of the considered of-the-shelf devices. Therefore, other efforts have investigated bit extraction mechanisms based on the whole channel impulse response. We briefly summarize some of these approaches in the next section.

4.1.5 CIR-based Key Generation

The received signal strength is an important indicator that characterizes the wireless channel and gives an insight on its reliability. However, the wireless channel has many other characteristics that can be used in the process of key generation. The channel impulse response is a more accurate representation of the wireless channel incorporating diversity and multipath. It can be accurately estimated at a wireless device by using appropriate reference signals. Therefore, many approaches target leveraging the channel impulse response in order to achieve high rate key generation. In the following, we describe briefly the recent work based on using the CIR to generate secret keys between wireless devices.

In this context, Wilson et al. [8] were one of the first to derive the secret key capacity in multipath channels. In their pioneering work, they derive an expression of the mutual information between the channel observations, which forms an upper bound on the secret-key rate. They also investigate the variation of this rate as a function of the signal bandwidth. Interestingly, it was found that the secret-key rate does not increase monotonically with bandwidth. Therefore, the authors have derived the optimal signaling bandwidth as a function of SNR for some typical UWB channel excess delays. In addition, the authors have investigated different public discussion methods and compared them through simulations.

Chunxuan et al. were also one of the first to investigate key extraction from multipath channels. In [67], they investigate key generation from jointly Gaussian random variables and derive the secret key capacity as a function of the received SNR. In addition, the authors propose a key generation mechanism based on applying an equally probable quantization scheme and an LDPC error correcting code for error reconciliation. Furthermore, they also compare gray coding and natural coding.

In [68], this key generation algorithm was further extended and applied on ITU channels [69]. In fact, wireless channel taps have been shown to have a complex Gaussian distribution [18]. Therefore, the authors have applied their approach on multipath wireless channels. They propose an Orthogonal Greedy Algorithm (OGA) for channel decomposition and extraction of channel taps. Then, they apply the quantization and error correction techniques in [67] to validate the key generation efficiency from typical multipath fading channels.

In [70], Sayeed et al. consider a simple block fading model where the frequency band is divided into D coherence bands. The authors consider the phase quantization of the channel coefficients in the different frequency bands which are assumed to be independent and identically distributed. The main contribution of this paper is the derivation of the probability of error as a function of SNR and the number of quantization levels. The authors also derive the minimum energy required for a successful acquisition of a secret key between two nodes.

In [9], Wallace investigates the theoretical limits of the secret key rate from multipath wireless channels in case the channel at the eavesdropper is correlated with that at the legitimate nodes. The author derives an expression of the secret key rate in function of the channel covariance matrices. Interestingly, it was found that from a security perspective channels with higher order of diversity (higher number of paths) are more suitable for secret key generation. The author also proposes an intelligent Channel Quantization mechanism with Guard bands (CQG) . It is mainly based on mitigating errors by the separation of the decision areas by guard bands.

This mechanism was further investigated in [71]. In their paper, Sun et al. analyze the performance of the CQG mechanism and derive expressions for the Bit Error Rate (BER) and the key generation efficiency. Moreover, the authors consider concatenating this protocol with reconciliation viewed as a Slepian-Wolf lossless compress coding [72]. They show that the key generation efficiency can be maximized by selecting appropriate guardband regions and LDPC code rates.

In [73, 74], another key generation mechanism called “Channel Quantization Alternating (CQA)“ was proposed. It is mainly based on using alternating staggered quantization maps instead of a guard band. Using simulations, this method has been proven to achieve a better performance than the direct quantization and the quantization with guard-band methods. Furthermore, the authors discuss the case of multi-antennas and investigate different rate error correcting codes.

Alternatively, a different attempt has been proposed by Chen et al. in [75, 76]. In their paper, the authors propose a MIMO-channel based encryption of a channel matrix, to be used to generate a secret key. The authors further discuss several error reduction techniques such as Gray coding, least-square estimation, channel averaging and LDPC codes.

In [77], a new method has been proposed for generating secret keys based on the common wireless channel. In this work, the authors do not quantize directly the phases of the channel taps. Instead, they consider sending random-phased beacons. These are then received at the legitimate node shifted by the random phase of the common channel. In other words, it is a kind of channel encryption of a chosen random phase value which will be consequently used to derive a secret key. Moreover, the authors propose using the channel multiple times even during the coherence period to achieve a high secret key generation rate. However, in appendix C, we prove that this method is not secure and any adversary in the communication range of the two nodes is able to deduce a correlation between the bits of the agreed-on key.

In addition to that, a relay-assisted scheme for key generation is proposed in [78, 79]. In this scheme, multiple relay nodes are employed to help increase the key generation rate. The authors derive expressions of the mutual information in addition to a more tight Cramer-Rao bound on the key rate. However, the security of such mechanism relies completely on the trustworthiness of the relay nodes.

Apart from that, Chou et al. [80] have studied the impact of channel sparsity and correlated eavesdropping on secret key generation from multipath wireless channels. In their work, the authors define a sparsity parameter ρ as the ratio of the subchannels having a non-vanishing independent coefficient, over the whole number of subchannels. Consequently, the authors derive the optimal sparsity that yields the maximum secret key capacity for a given SNR. Moreover, they tackle the issue of a correlated eavesdropper and investigate the effect of correlation with an eavesdropper's channel measurements on the secret key capacity.

As for the case of Frequency Division Duplex (FDD) systems, key generation from the wireless multipath channel was investigated by Wang et al. in [81]. The authors argue that despite the non-reciprocity of the channel impulse response, some parameters can be used for generating a common secret key. They consider that the multipath angles and the time delays of the multipath components are reciprocal parameters that can be used in generating secure keys. They propose a key generation mechanism based on quantizing these parameters, and a reconciliation stage by performing error correction based on the Chinese Remainder Theorem (CRT).

4.1.6 Miscellaneous Key Generation Mechanisms

Apart from the channel impulse response or the received signal strength, there have been other several approaches proposed to generate secret keys based on some properties of the physical layer of wireless communication. Kitano et al. [82] have investigated secret key generation based on the fluctuations of the BER in wireless communications. The authors argue that BER is an appropriate indicator to characterize the wireless channel as it incorporates the different factors that lead to bit errors, such as fluctuations of amplitude and phase, and the effect of multipath and delayed waves.

Tsouri et al. [83] have proposed a reverse piloting protocol. The main idea of this protocol is the transmission of pilot signals by the receiver so that the transmitter can estimate the channel and compensate it during the transmission through a coding scheme. As a result, the channel performs an automatic symbol level encryption. The authors analyze this key generation mechanism and derive the relation between the efficiency of the source, the coherence bandwidth and the Doppler bandwidth. As for the secrecy of this protocol, the authors argue that an eavesdropper cannot have an accurate estimate of the channel and can only perform blind estimation since the transmitter does not send any pilots or reference signals. However, any known transmitted message (for example the synchronization signal) can be leveraged by the eavesdropper to estimate the channel and break the secrecy of the derived key. Therefore, this protocol needs further investigation to prove its security.

A random channel hopping scheme for key agreement in wireless networks has been proposed by Zan et al. in [84]. In this scheme, the transmission of data is based on choosing a random hopping sequence. On the other hand, the receiver also listens on a random chosen channel; and when it hears a packet, it sends an acknowledgment. Hence, the received bit pattern will be used to establish a key. The authors have analyzed this approach and derived the average number of trials to reach key agreement and elaborated the probability of error of an adversary. However, the security of this mechanism is based on the assumption that the adversary is not able to listen to all channels simultaneously. Therefore, this key generation mechanism is not secure against a powerful adversary.

Gollakota et al. [31] have proposed a channel-independent method for secret key agreement based on reactive jamming by the receiver. The method called iJam works as follows: The transmitter transmits 2 OFDM symbols while the receiver jams randomly half the time samples of each so that an eavesdropper will get a jammed signal. On the other hand, the jamming receiver knowing the jamming sequence will combine the non jammed samples to get a jamming-free OFDM symbol. The authors have further investigated different modulations and enhanced the effectiveness of this mechanism against eavesdroppers in different locations making their mechanism location independent. Finally, the results of their testbed implementation showed that their method has a secrecy rate of $3 - 18$ Kb/s with a 0% bit disagreement.

4.1.7 Physical-layer Authentication

Recently, it has been found that some parameters of the physical layer can be used to authenticate wireless devices. While some have investigated using hardware signatures and clock skews as fingerprints [85], the wireless channel characteristics have been largely explored as a physical fingerprint [30, 85, 86, 87]. In Chapter 3, we have seen that the wireless channel effects change according to the location of the wireless node in a rich scattering environment. Therefore, this property can be used to authenticate a wireless device according to its position.

4.1.7.1 Static Environment

When the environment is static, the channel characteristics remain constant with time. This property can be used to authenticate a wireless device according to its location. Moreover, the authentication according to the channel impulse response or consequently the location can be used as a countermeasure against Sybil attacks or Identity-theft attacks.

In a Sybil attack, an adversary creates a number of virtual or pseudonymous entities to gain a disproportionally large influence on the system or to gain a larger portion of the available resources. Hence, an authentication scheme based on the location can identify the virtual identities as corresponding to one physical identity and therefore identify the attacker.

An adversary can also perform an Identity-theft attack where it steals the identity of another entity and sends erroneous data in the name of this entity. Hence, an authentication based on the wireless channel impulse response and location can identify that the communicating entity is indeed who it claims to be or not.

4.1.7.2 Mobile Environment

When the environment is mobile, the channel characteristics vary with time. Hence, the channel impulse response cannot be used for instantaneous authentication of an entity. However, this provides a method towards continuous authentication. This means that whenever an entity is authenticated, it can be continuously tracked and we can ensure if it is always the same communicating entity or not. In fact, the channel varies continuously with time but stays correlated in relatively short periods and hence can be tracked. In this case, it is important to calculate the autocorrelation function between the channel impulse responses at different time instants. Therefore, a high or low correlation of the channel in a small time interval proves if the node is indeed who it claims to be or not.

4.2 System Model

4.2.1 General System Model

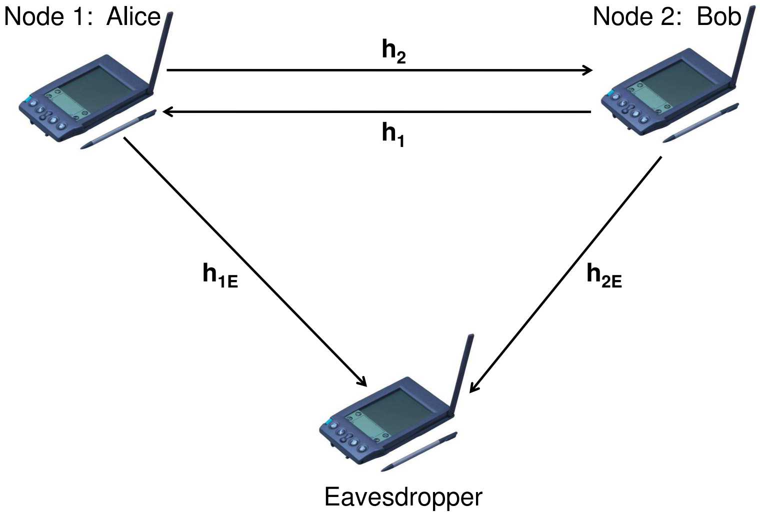


Figure 4.1: A wireless communication scenario consisting of two legitimate communicating nodes and an eavesdropper.

In this section, we describe the general system model which is formed mainly of two communicating nodes Alice(Node 1) and Bob(Node 2) and an eavesdropper (Eve) as shown in Fig. 4.1. In this scenario, Alice and Bob want to derive and agree on a secret key that can be used to secure their communication. This key should be secure in a way that Eve or any other eavesdropper should not get any information about this key.

We suppose also that Alice and Bob are using the same frequency band (i.e. Time Division Duplex communication) so that they are experiencing the same channel. Moreover, we assume that Eve is sufficiently separated in space so that her channel observations are completely uncorrelated from those of Bob and Alice. In fact, multipath wireless channels are characterized by their fast variation with location such that in locations separated by even small distances in the order of a wavelength, a different channel is experienced. As a result, the two channels $\mathbf{h_1}$ and $\mathbf{h_2}$ are practically different from the channel observations of Eve. And due to the reciprocity principle, they are equivalent. Hence, they can be leveraged in extracting a shared secret key.

4.2.2 Multipath Channel

The wireless channel considered in this scenario is supposed to be a multipath fading channel which can be modeled as a combination of different channel impulses (channel taps) having different amplitudes and delays. In fact, the channel incorporates the different paths which are traversed by the signal traveling from the source to the destination. Each of these channel taps is characterized by its complex gain and delay. In addition, due to the mobility of the communicating nodes and the reflecting clusters, the channel is varying with time. In other words, the channel impulse response at time instant t can be expressed as

$$h(t,\tau) = \sum_{l=0}^{L-1} h_l(t)\delta(\tau - \tau_l), \tag{4.3}$$

where δ is the unit impulse function, L is the length of the channel (number of taps), while $h_l(t)$ and τ_l represent the complex gain and delay of the $(l+1)^{th}$ channel tap at time instant t.

The main idea in this work is to use the wireless channel as a source of secret information. The channel taps can be considered independent from each other and can be quantized separately thus leveraging multipath to increase the number of secret bits generated [9, 68, 88, 89]. Moreover, the uniform phase distribution [18] of the channel taps encourages the idea of phase quantization to generate secret keys. In fact, a condition of secrecy is the perfect randomness. Thats why we tend to use the randomly distributed phase to generate secret bits.

It is important to note that the variation of the channel with time can have a negative influence on the performance of a key extraction mechanism. Channel variation influences negatively the channel estimation procedure. Therefore, the channel estimation procedure should be done at the two nodes as fast as possible to avoid any decorrelation between the channel estimates.

However, due to some practical issues, it is difficult to obtain channel estimates at the same instant. Thus, in the case of small delay and mobility, the resulting channel variation should be modeled and corrected as we will see in section 4.4.2. In deed, Basis Expansion Modeling (BEM) [90] has been largely investigated to model channel variation during short periods where the channel is highly correlated. In this case, it is important to find the time-spaced autocorrelation function as it determines the channel correlation as a function of time-shift Δt. Hence, it is necessary to take into account the coherence time of the channel and the autocorrelation function as these parameters help in determining how much the channel is correlated.

Moreover, the phase of the channel taps is very sensitive to time synchronization and frequency offset. Indeed, a small residual frequency offset might lead to a considerable variation in the estimated phase of the channel taps and would result in a disagreement between the extracted bits. However, in this work we assume perfect time and frequency synchronization and leave these issues to be handled in future work with real implementations and testing.

4.2.3 Channel Estimation

Channel estimation is a necessary part of a digital signal processing unit of any radio device. It helps in performing equalization and error correction. In our case, it is necessary to perform accurate channel estimation so that the channel estimates could be used to derive and agree on a key. In this section, we briefly summarize the channel estimation procedure in an OFDM (Orthogonal Frequency Division Multiplexing) system.

One of the main advantages of an OFDM system is that it allows a simple channel estimation. In deed, the FFT (Fast Fourier Transform) and IFFT (Inverse Fast Fourier Transform) allows the transformation of the channel matrix into a diagonal matrix in the frequency domain. Hence, considering an OFDM system, the channel coefficients in the frequency domain can be estimated by a simple division obtaining [90]:

$$\widehat{\mathbf{H}} = \mathbf{H} + \mathbf{n_G}, \tag{4.4}$$

where $\mathbf{n_G}$ is the added white Gaussian noise vector which can be different at the two nodes; and $\mathbf{H}$ is a vector of N channel coefficients in the frequency domain with N being the FFT size. These channel coefficients can be expressed as (taking out the time index t)

$$H_k = \frac{1}{\sqrt{N}} \sum_{l=0}^{L-1} h_l \exp\left(\frac{-j2\pi kl}{N}\right) \tag{4.5}$$

The basic idea is to use these channel coefficients to derive secret bits. Hence, a direct approach that comes first in mind is quantizing these coefficients directly. However, the channel coefficients show some correlation in the frequency domain. Therefore, we tend to transform them to the time domain where we get the uncorrelated channel taps. In our approach, we first estimate the H_k's and then by Fourier transform we obtain the h_l's as:

$$\widehat{\mathbf{h}} = \mathbf{h} + \mathbf{z}, \tag{4.6}$$

where $\mathbf{z}$ is the equivalent Gaussian noise in the time domain.

Since the Fourier transform is a unitary transform, Parseval's theorem states that:

$$\sum_{l=0}^{L-1} |h_l|^2 = \sum_{k=0}^{N-1} |H_k|^2 \tag{4.7}$$

Therefore, we have the following relation between the frequency domain SNR: $SNR_f = E[|H_k|^2]$ and the SNR of the time domain channel coefficients: $SNR_\tau(l) = E[|h_l|^2]$:

$$\sum_{l=0}^{L-1} SNR_\tau(l) = N \cdot SNR_f \tag{4.8}$$

This means that the use of N channel samples in the frequency domain to find the time domain coefficients leads to a gain of Tap-to-Noise power Ratio (TNR) equal to N.

4.2.4 Key Agreement Protocol

The communicating nodes need only to estimate their common channel to be able to generate a secret key. It is also very important to perform this estimation in a very short period, especially in mobile scenarios where the channel response varies rapidly. Therefore, the first step in the key generation procedure should be the consecutive exchange of probe or pilot signals so that the two nodes can obtain accurate channel estimates.

We propose a simple key generation protocol consisting mainly of channel estimation, exchange of quantization parameters, quantization and secret bit extraction, and finally key agreement and verification. Considering, without loss of generality, that Node 1 is the leading node and Node 2 is the follower, we summarize the key generation and agreement protocol in the following steps:

1. Node 1 sends a pilot signal to Node 2 for the purpose of channel estimation.

2. Node 2 sends back a pilot signal to Node 1 for the purpose of channel estimation.

3. Nodes exchange parameters (ex. TNRs, Tap Indexes,...) related to the key generation mechanism over the public insecure channel. The purpose of this exchange is to minimize the probability of disagreement without any loss of secrecy. The parameters exchanged vary according to the key generation protocol as we will see in section 4.3.

4. Nodes proceed in quantizing channel taps according to the key generation mechanism.

5. Steps $1 - 4$ can be repeated as necessary, consecutive times for performance enhancement or larger key sizes.

6. Verification of agreement on the derived key (e.g. sending hash values, encrypted nonces). In this step, the nodes have to verify that they actually derived the same key and there is no error in the key extraction process.

4.3 Proposed Key Generation Mechanisms

In this section, we first present the direct quantization approach consisting of direct quantization of all channel taps. We discuss why this approach leads to a high error rate implying the need of error correcting codes, information reconciliation and consequently privacy amplification. After that, we present our proposed key extraction approaches. Our proposed approaches target minimizing the probability of error during the quantization stage. Basically, we analyze the origin of error and propose two methods. One is based on mitigating error by avoiding quantizing channel taps which are prone to error. Whereas, the other is based on shifting the random phases of channel taps toward the modulation constellation points.

4.3.1 Drawbacks of Direct Quantization

The direct approach consists of directly quantizing the phases of the obtained channel taps through a normal Phase Shift Keying (PSK) demodulation procedure. In other words, the obtained channel estimates and the the quantization precision (number of quantization levels) are input to a PSK demodulator which outputs the extracted bits. However, this direct quantization leads to a high percentage of error as we will see later in the simulation results.

In Fig. 4.2, we show a plot of a number of channel realizations over the complex plane and their noisy estimates. We see that the added Gaussian noise leads to a shift of the channel gains, which depends on the TNR. This leads to a high probability of error in case a channel complex gain is very close to the border line between the decision regions. If we consider, for example, a QPSK demodulation (four decision regions), we can see clearly that the points close to the axes are the most prone to error. Even a small noise can cause a channel tap to be shifted from one region to another. Therefore, an intelligent quantization approach should either avoid quantizing these values (using guard intervals separating the different quantization regions), or shift the random channel gains to be concentrated around the constellation points apart from the border regions (a phase shifting approach).

4.3.2 Guard Intervals Method

As we have discussed above, it is obvious that the high error rate is mainly due to the channel values close to the border regions. Therefore, we propose a method to mitigate

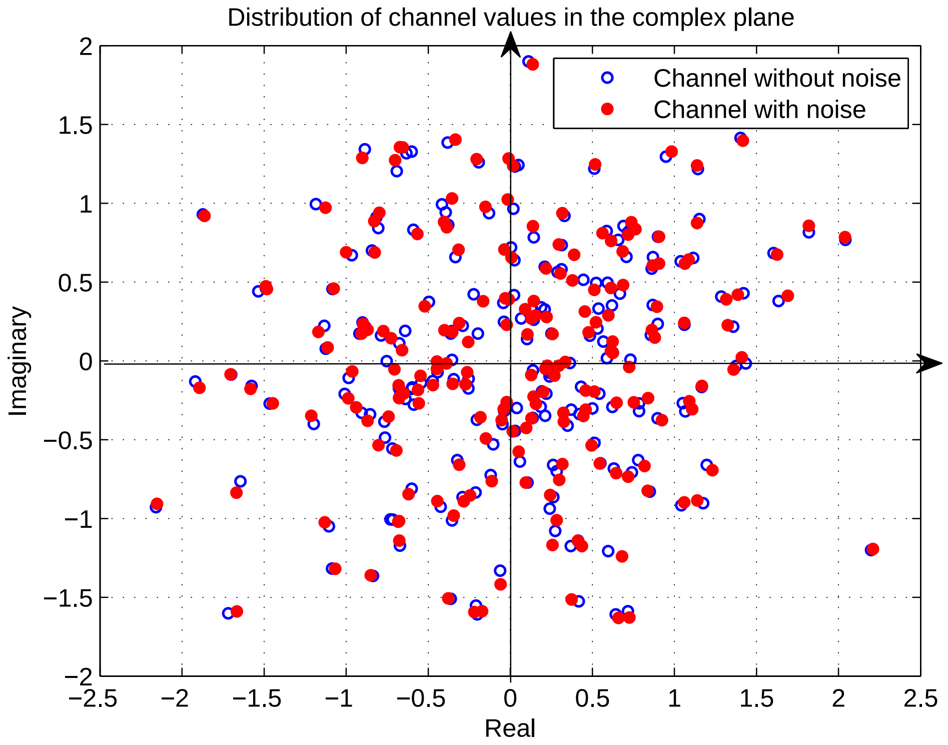


Figure 4.2: A distribution of some channel realizations and their noisy estimates over the complex plane.

error based on separating the quantization regions by small boundary regions. These guard bands allow to avoid the channel values that may cause a disagreement between the two communicating nodes.

In our key generation mechanism, we investigate extracting secret bits through the quantization of the phases of the channel taps. Hence, we define the boundary regions by guard phase intervals such that if the channel tap phase lies in one of these intervals, it is simply discarded and not used in the key generation process.

From a security point of view, one may think how each node can inform the other that a channel tap should be discarded without any loss of secrecy. In fact, as the quantization regions are equiprobable, so are the boundary regions. In this case, any node can just announce during the public discussion phase which channel taps to be quantized or which to be discarded. In our approach, the leader node first announces its accepted channel taps by sending the corresponding indexes and so does the follower back. Thus, they agree on the channel taps to be used in the secret bits extraction process.

As for the performance, it is clear that larger boundary regions leads to a lower probability of bit disagreement but also a lower number of bits extracted since more channel taps are likely to be discarded. Thus, a performance-efficiency trade-off can be made in this case. In fact, using guard intervals increases the reliability of the generated secret key at the expense of a lower efficiency. Therefore, we consider a certain target probability of key disagreement and aim at extracting the maximum number of secret bits. In particular, we consider a target disagreement *per channel tap* to be less than 10^{-3} and we seek the optimal guard angle and quantization level achieving the maximum number of secret bits.

In Appendix B, we derive the probability of disagreement as a function of the guard angle β, the quantization level M, and the tap-to-noise ratio TNR as:

$$P_{GI} = \frac{1}{\pi/M - \beta/2} \cdot \int_{\theta=0}^{\theta=\pi/M-\beta/2} P_\theta(\beta, M, \sigma) d\theta, \tag{4.9}$$

where P_θ is given by:

$$P_\theta = \frac{1}{2} \cdot [1 - \mathrm{erf}(\frac{1}{\sqrt{2}\sigma} \tan(\frac{\pi}{M} - \theta + \frac{\beta}{2}))], \tag{4.10}$$

On the other hand, the average number of bits generated per channel tap depends also directly on β and M. The probability that the channel tap does not lie in the guard interval and is used in the secret bit extraction process:

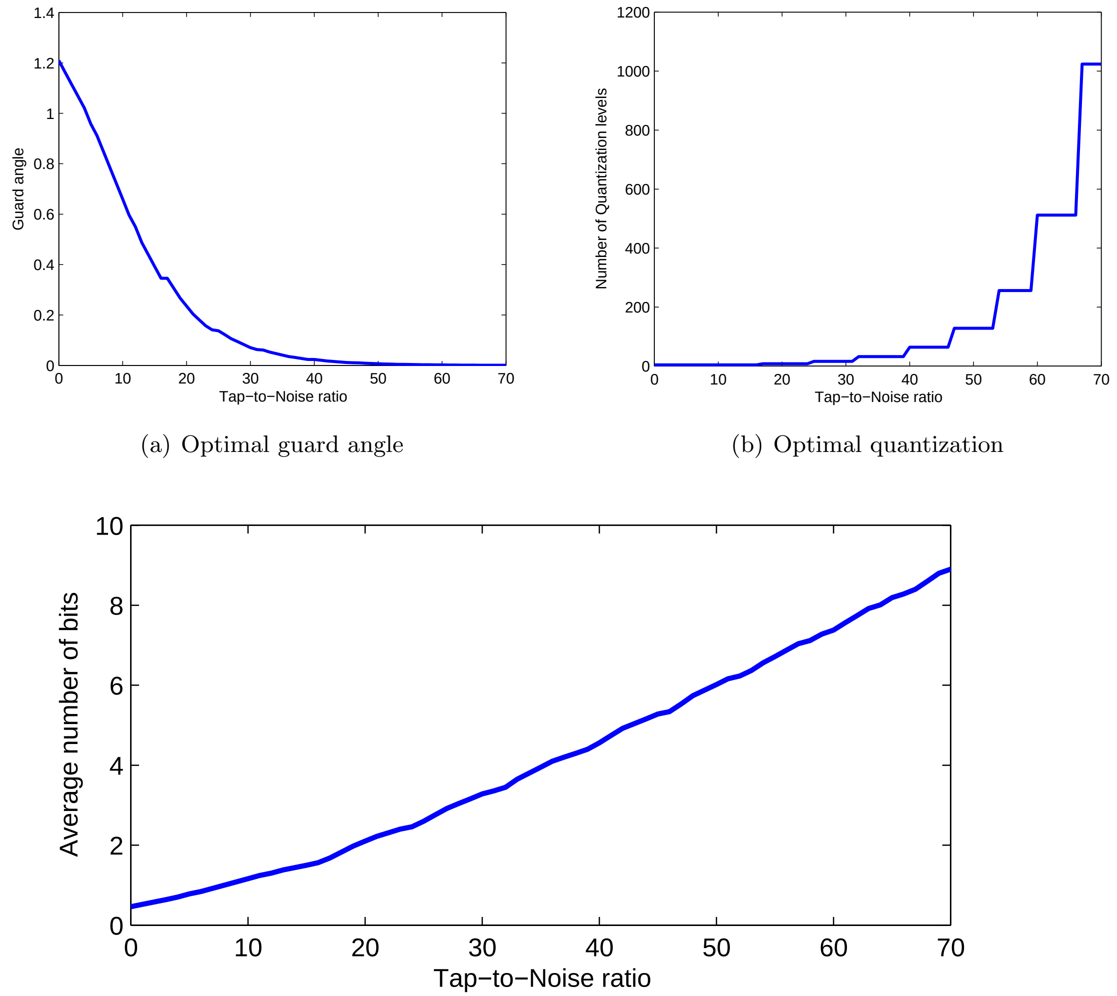
$$P(h_l \notin GI) = (1 - \frac{\beta \cdot M}{2\pi}) \tag{4.11}$$

Hence, the average number of secret bits generated from a channel tap can be found to be upper bounded by:

$$N_{av} \leq (1 - \frac{\beta \cdot M}{2\pi}) \cdot \log_2(M), \tag{4.12}$$

From (4.9), we proceed in computing the probability of error in function of TNR for different values of β and M. Then, by considering the threshold probability of error of 10^{-3} per channel tap, we derive the optimal parameters achieving the highest number of secret bits generated as shown in Fig. 4.3.

As a result, the public discussion phase includes in this case exchanging the quantization parameters (number of quantization levels) and the indexes of the channel taps to be taken into account in the key generation process. It is clear that this exchange has no drawbacks on the secrecy of the derived key as the transmission of the TNR values does not decrease the entropy of the phases of the channel taps which have a random distribution [18].



(a) Optimal guard angle

(b) Optimal quantization

(c) Average number of bits generated

Figure 4.3: Optimal guard angle (a), number of quantization levels (b), and average number of bits generated per one channel tap (c) as a function of TNR for a probability of error < 0.001, Guard Intervals (GI) method.

4.3.3 Phase Shifting Method

From eq. (4.12), we can deduce that the guard intervals mechanism is not optimal in the sense of the efficiency of key extraction. In this approach, channel values lying in the guard intervals are simply ignored and not included in the quantization process.

This leads to a decrease in the average number of secret bits extracted by a factor equal to $\beta M/2\pi$.

Therefore, to achieve a higher efficiency of key extraction, the whole channel response should be considered. In other words, no channel taps with sufficient TNR should be ignored. Therefore, we propose a new approach to mitigate errors in channel quantization. It is mainly based on shifting the phases of the channel taps in a synchronous way between the two nodes approaching the demodulation constellation. The idea is mainly to convert the problem into a normal demodulation problem where the channel values are spread around the constellation points rather than being randomly scattered. Hence, a direct quantization can be performed without the need for guard intervals.

To clarify this procedure, lets consider h_1 as a 1-tap channel estimate at Node 1 and h_2 as a 1-tap channel estimate at Node 2. In this approach, Node 1 first quantizes its channel tap value by a proper PSK demodulation and then sends during the public discussion phase, the phase difference $\mu = \theta_1 - \hat{\theta}$ to the other node, where θ_1 is the phase of h_1 as estimated at Node 1 and $\hat{\theta}$ is the phase of the obtained constellation point after PSK demodulation.

We suppose always that a reliable channel exists for the transmission of μ to Node 2. Consequently, Node 2 corrects its own estimated channel tap phase as:

$$\theta_2' = \theta_2 - \mu = \theta_2 - \theta_1 + \hat{\theta}, \tag{4.13}$$

where θ_2 is the phase of the corresponding channel tap h_2 as estimated by Node 2.

We can also write (4.13) as:

$$\theta_2' = \Delta\theta + \hat{\theta}, \tag{4.14}$$

where $\Delta\theta = \theta_2 - \theta_1$ represents the combined effect of noise.

From a security point of view, one may wonder how secure is this approach and if it causes any loss of secrecy. In fact, as the phases of the channel taps are random and uniformly distributed, then the transmission of a phase shift over the public channel does not reveal hazardous information about the corresponding phase. This provides an eavesdropper only with the information that the phase of the channel tap is μ away from a constellation point. But since the constellation points are equiprobable, no additional information is provided to the eavesdropper. Hence, the public discussion phase consists of transmitting the phase shifts, measured TNR values and indexes of the channel taps to be quantized, i.e. those with sufficient TNR.

As for the performance, an error only occurs in the key extraction process if $|\Delta\theta|$ is large enough, i.e. if $|\Delta\theta| > \pi/M$. In Appendix B, we derive the probability of disagreement for quantizing one channel tap as a function of the tap-to-noise power ratio and the number of quantization levels M in the case of high TNR and low TNR.

Based on this formulation, we develop similarly as in the GI mechanism, an adaptive quantization algorithm where the number of quantization levels varies depending on the tap-to-noise power ratio. We target achieving a certain probability of error per channel tap and seek the maximum number of quantization levels. Thus, by considering a probability of disagreement per channel tap less than 10^{-3}, we obtain the **optimal** number of quantization levels as a function of TNR as shown in Fig. 4.4.

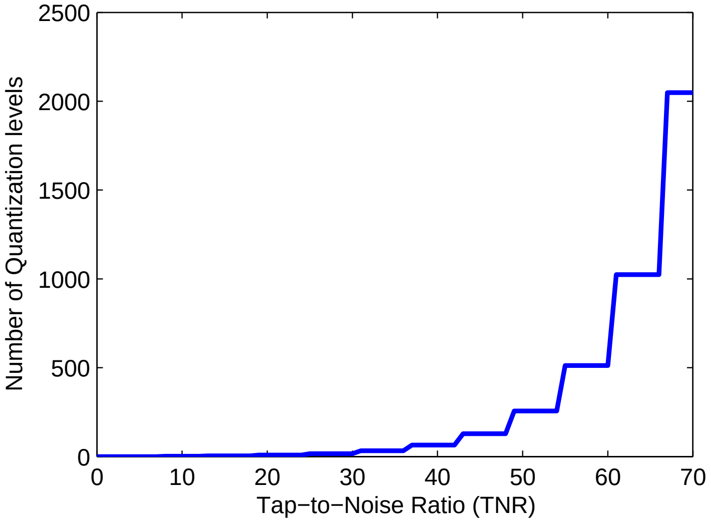


Figure 4.4: Optimal number of quantization levels as a function of TNR for a probability of error per channel tap < 0.001, PS approach.

Comparing this graph to that in Fig. 4.3, we can observe that the PS mechanism is more efficient than the GI mechanism. In section 4.3.5, we prove out this point through Monte Carlo simulations.

4.3.4 Further Improvements

As we have seen through the previous sections, the performance of the key extraction methods depend on the tap-to-noise ratios of the different channel taps. Indeed, in our adaptive quantization approach, the number of quantization levels (consequently number of secret bits) depends on the TNR. Hence, enhancing the TNR of the channel taps is beneficial for the key generation procedure. One of the possible solutions proposed is to average multiple channel observations in the time domain. Indeed, averaging over multiple observations leads to an increase of the TNR proportional to the number of observations considered.

On the other hand, we have seen in Section 4.2.3 that the sampling of the channel in the frequency domain and then the transfer to the time domain leads to a gain in the TNR equal to N. In addition, higher sampling rates enables more channel taps to be considered. With higher sampling, some channel taps which are normally non-revocable become revocable and can be incorporated separately in the key generation procedure. Therefore, the use of higher FFT sizes and bandwidths may also lead to a higher secret bits extraction rate.

4.3.5 Simulation Results

Our system follows the IEEE 802.11n standard [91]. In particular, we consider a 20 MHz bandwidth divided over 64 subcarriers and we consider TDD communication. The duration of each OFDM symbol is $3.2\mu s$ in addition to a cyclic prefix up to $1.6\mu s$. As for the channel model, we test our algorithms on one of the channel models defined by IEEE 802.11 Task Group n TGn [17]; particularly, we use the Model F which is defined as a large space indoor or outdoor channel model. We consider in our simulations a Single Input Single Output (SISO) channel and we test our algorithms in terms of the number of secret bits extracted from a single channel observation. We further express the results of our algorithms in terms of the probability of disagreement and the average number of bits generated as a function of SNR, where SNR stands here for the received signal-to-noise ratio. In fact, there is an efficiency-performance trade-off. Hence, we target a certain probability of disagreement of the derived key, i.e. the probability that there is no error in any bit extracted. Particularly, we target a probability of error *per one channel tap* to be below 10^{-3}.

In Fig. 4.5, we trace the probability of disagreement of the derived key stream as a function of SNR for the direct quantization approach, the guard-intervals approach and the phase shifting one. For the direct quantization approach, we observe a high probability of disagreement which makes it a non-reliable approach. As for the guard-intervals and the phase shifting methods, we observe a much lower probability of disagreement in the order of 10^{-2} and 10^{-3} respectively.

Further, in Fig. 4.6, we compare the average number of secret bits extracted by the phase shifting method as a function of SNR with that of the guard intervals method. It is obvious that the PS mechanism outperforms the guard intervals mechanism, as it yields a larger number of secret bits extracted. For example, for an SNR higher than 40dB, PS leads to the extraction of more than 90 secret bits compared to 60 for the GI method. We also compare the maximum and minimum number of bits extracted. Interestingly, the GI method shows a much bigger deviation from the average where the minimum number of extracted secret bits is equal to zero. This is due to the fact that in the guard-intervals key generation method, many channel taps lying in the guard intervals are being simply ignored and there is a non-vanishing probability that all channel taps lie in the guard intervals.

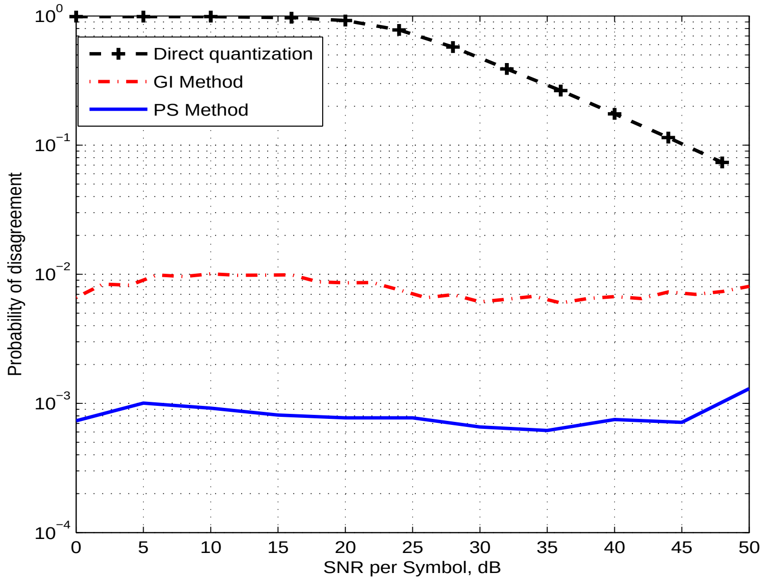


Figure 4.5: Probability of disagreement as a function of SNR for the three approaches, N=64.

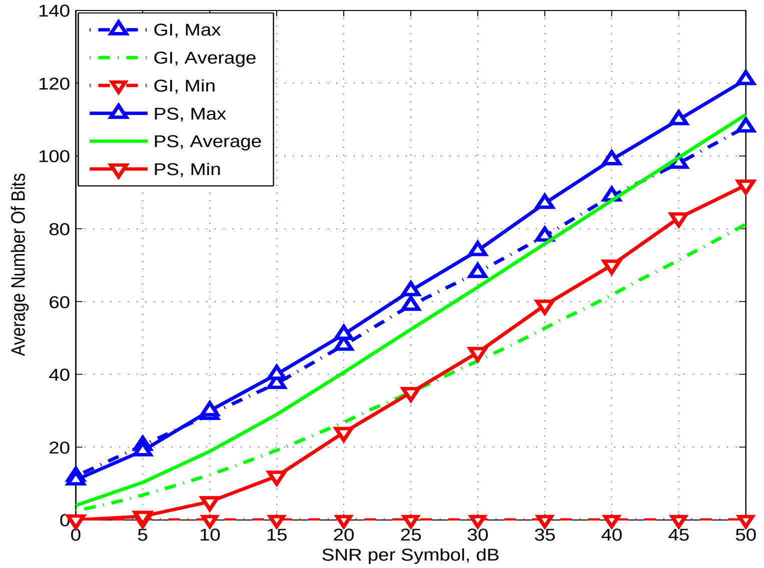


Figure 4.6: Average, maximum, and minimum number of bits generated as a function of SNR, N=64.

In Fig. 4.7, we show the average number of secret bits extracted by the phase shifting method by averaging over multiple OFDM symbols. In this case, the communicating nodes send multiple pilot OFDM symbols for the purpose of channel estimation rather than sending only one OFDM symbol, thus obtaining an average over multiple channel observations. We observe here that the higher the number of OFDM symbols used, the higher the number of secret bits extracted. Comparing the case of 5 OFDM symbols sent by each node to that of 1 OFDM symbol, we can observe an improvement of approximately 7 dB.

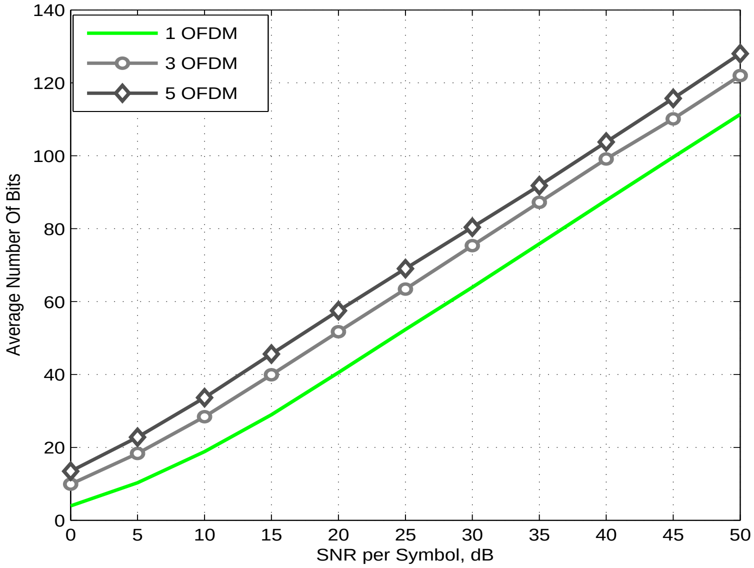


Figure 4.7: Average number of bits generated by averaging over multiple OFDM symbols as a function of SNR, PS method, N=64.

Finally, in Fig. 4.8, we show the results for various FFT sizes (64, 128 and 256) and bandwidths (20MHz, 40MHz, and 80MHz respectively). We observe that higher FFT sizes and larger bandwidths lead to a higher number of secret bits extracted as predicted in Section 4.3.4. In fact, better TNRs are obtained for higher FFTs since the TNR is proportional to the FFT size. Moreover, higher sampling rates enable more channel taps (which are non-resolvable at lower sampling rates) to be taken into account which leads to a higher number of secret bits extracted.

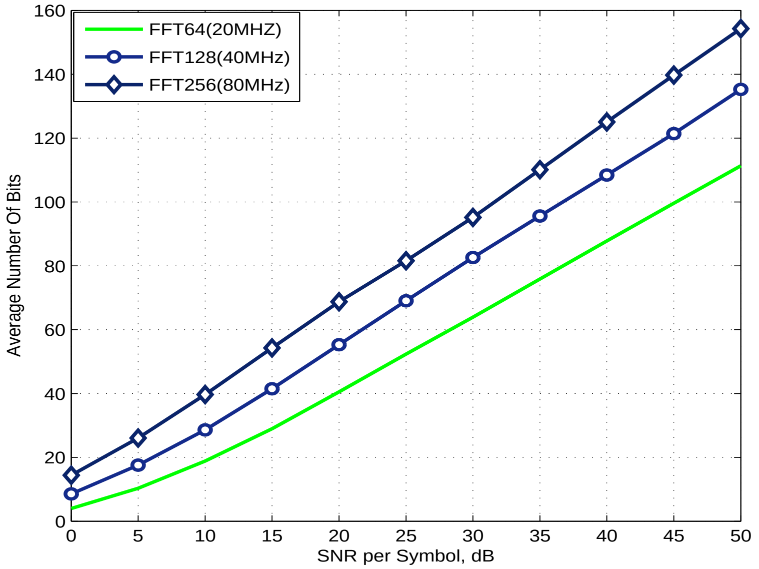


Figure 4.8: Average number of bits generated as a function of SNR for various FFT sizes, PS method.

4.4 Practical Issues

In this section, we investigate some practical issues that affect the performance of key generation from the multipath wireless channel. First of all, we discuss synchronization and frequency offset issues and highlight the necessity of time and frequency synchronization. After that, we study the effect of delay between the channel estimates on the performance of the key generation mechanism. Based on the results, we propose a modification to the key extraction mechanism to mitigate the performance degradation due to delay. Finally, we investigate the effect of channel variation and decorrelation due to mobility on the performance and improve our proposed key generation mechanism accordingly.

4.4.1 Synchronization and Frequency Offset

Time and frequency synchronization are very important requirements in a wireless key generation mechanism. Basically, key generation from wireless multipath channels is based on the principle of reciprocity of the channel. Hence, any time or frequency offset might lead to a higher probability of disagreement between the generated keys. In fact, a small residual frequency offset might lead to a considerable variation in the estimated phases of the channel taps and would result into a disagreement between the generated keys. Therefore, it is very important to have a high time and frequency synchronization in a wireless key generation system.

In this work, we assume perfect time and frequency synchronization. Hence, we do not consider any time synchronization issues and we assume a zero frequency offset. These issues are then left to be handled in future work with real implementations and testing.

4.4.2 Robustness to Delay: The 3-Way PS Mechanism

4.4.2.1 Effect of Delay

As mentioned before in the key agreement protocol, it is important that the channel estimation occurs at the two nodes in a short period. Otherwise, the variation of the channel results into different channel estimates at the two nodes. However, the delay between channel estimates is very difficult to avoid. There are many reasons that might result in delaying the channel estimation at the other node. Mainly, we can mention: transmission delay (in the order of few microseconds), transmit-to-receive-switch delay (less than 5 microseconds), in addition to other protocol related factors (for example the minimum physical frame size).

To study the effect of delay on the performance, we vary the delay between the channel estimates from a range of $5\mu s$ (the minimum practical delay) to $250\mu s$. Fig. 4.9 shows the probability of disagreement as a function of the delay between both channel estimates for an SNR of 30dB. Observing the solid line, we can state clearly that as the delay between the channel estimates increases, the probability of disagreement increases significantly. This is mainly due to the varying nature of the channel.

However, for such considered delays the channel is still highly correlated. In fact, the coherence time (for an autocorrelation > 0.75), normally approximated as: $\tau_C = \frac{1}{2\pi f_D}$, is, in this case, in the order of few milliseconds while the delay is in the order of microseconds. This means that it is possible to correct the channel gains and mitigate the phase variation. In the following section, we propose a modification to the secret bit extraction mechanism to mitigate the effect of the variation of the channel gains during short periods of high correlation.

4.4.2.2 3-Way PS Mechanism

In this section, we improve the robustness of the key generation mechanism against delay between the channel estimates. As discussed above, during the considered delays the channel is highly correlated. Hence, it is possible to correct the phases of the channel taps and remove the effect of channel variation.

To accomplish this task, we model the variation of the channel according to a BEM. Particularly, we model the channel variation as a polynomial of the first order, i.e. a

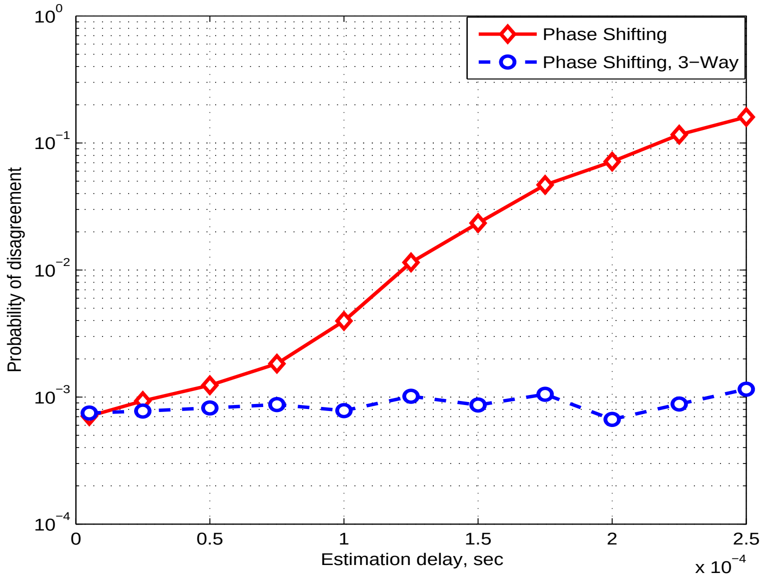


Figure 4.9: Probability of disagreement as a function of the delay between the channel estimates, SNR=30dB, N=64.

linear modeling, since the normalized Doppler spread is relatively small in this case [90]. Yet, this requires two channel estimates at different time instants to compute the modeling coefficients. Thus, we modify our key generation and agreement protocol to be based on a 3-way channel estimation mechanism.

This works as follows: Node 1 transmits a reference signal (Pilot OFDM symbol) to Node 2 at time instant t_1 for the purpose of channel estimation. Node 2 transmits back also a reference signal at time instant t_2 so that Node 1 can obtain an estimation of the channel impulse response. Finally, Node 1 retransmits another reference signal back at time instant t_3. In this case, Node 1 obtains a channel estimate at time instant t_2 while Node 2 would obtain two channel estimates at instants t_1 and t_3. As a result, Node 2 can now use these two channel estimates at two different time instants and compute the modeling coefficients. Thus, a modeling function can be used to calculate an estimate of the channel gains at the same instant t_2 when Node 1 would have obtained a channel estimate. Applying a linear modeling, Node 2 can calculate the estimate of $h(t_2)$ using the following equation:

$$\hat{h}(t_2) = h(t_1) + \frac{t_2 - t_1}{t_3 - t_1} \cdot (h(t_3) - h(t_1)), \tag{4.15}$$

We test this algorithm on the same system as before and for the different values of delay between the consecutive channel estimates. The dotted line in Fig. 4.9 shows the probability of disagreement as a function of delay for the 3-way PS mechanism. We can observe that the 3-way PS mechanism is robust to delay between the channel estimates. We obtain a probability of disagreement in the order of 10^{-3} as intended in our algorithm optimization while achieving an average number of 67 secret bits generated from a single channel observation at an SNR of 30dB.

4.4.3 Robustness to Mobility: The Enhanced 3-Way PS Mechanism

4.4.3.1 Effect of Mobility

In the discussion above, we have only considered the case of low mobility to study the effect of delay between the channel estimates. However, the variation of the channel leading to the degradation of performance in case of delay is mainly due to the mobility of the communicating nodes and reflecting clusters. Hence, it is necessary for a key generation mechanism to be robust against mobility. In this section, we study the effect of mobility on the performance of the key extraction mechanism and present an enhancement to the 3-way PS mechanism providing robustness against mobility and channel variation.

In fact, the channel variation can be partially corrected by the 3-way mechanism presented above. However, higher mobility leads to a faster decorrelation of the channel such that the channel estimates obtained at the two nodes are affected by a partial decorrelation in addition to the phase variation. And on the other hand, it leads to a bigger error in the polynomial modeling procedure.

Fig. 4.10 shows the probability of disagreement as a function of Doppler spread for an SNR of 30dB and a delay between the channel estimates of $250\mu s$[1]. The solid line corresponds to the 3-way mechanism discussed above. We observe clearly that higher mobility leads to a significant increase in the probability of disagreement.

4.4.3.2 Enhanced 3-Way PS Mechanism

In this section, we propose a mobility-resilience enhancement to the 3-way phase-shifting mechanism to mitigate the effect of channel decorrelation and the modeling error due to mobility. The idea is to approximate the channel decorrelation and deviation from the linear model as an added noise. However, it is difficult to calculate the exact value of this noise. Therefore, we approximate it as an added Gaussian noise with a variance expressed in function of the normalized Doppler spread ν_D as:

$$\sigma_D^2 = \frac{3}{2} - 2 \cdot J_0(2\pi\nu_D) + \frac{1}{2} \cdot J_0(4\pi\nu_D), \tag{4.16}$$

[1] A very high delay is considered to guarantee the robustness of the proposed solution against lower delays.

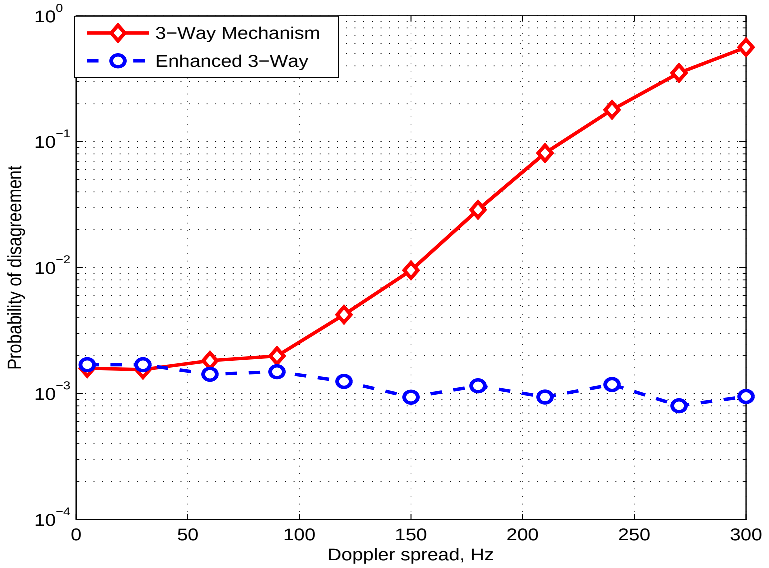


Figure 4.10: Probability of disagreement as a function of the Doppler spread (250μs delay), SNR=30dB, N=64.

The dotted line in Fig. 4.10 shows the probability of disagreement by using the Enhanced 3-way PS mechanism. We observe that this mechanism mitigates the error due to mobility and achieves the aimed probability of disagreement in the order of 10^{-3}.

In Fig. 4.11(a), we plot the average number of secret bits generated as a function of the Doppler spread using the Enhanced 3-way PS mechanism. We can observe that mobility has a negative effect on the number of secret bits generated from a single channel observation, as it decreases from 67 secret bits for a Doppler frequency of 5 Hz to less than 45 secret bits for a Doppler frequency of 300 Hz. This is mainly due to the decorrelation of the channel which leads to more noisy estimates.

4.4.4 Effect of Mobility on Overall Performance

Channel variation due to mobility has a negative effect on the performance of the key generation mechanism corresponding to a single channel observation. However, the effect of mobility on the overall performance, i.e. the key generation rate (measured in sbits(secret bits)/sec) is not clear yet. Therefore, one may still ask: Is mobility an advantage or a disadvantage for the key generation procedure?

To answer this question, we investigate the overall performance as a function of the Doppler spread. We should note that higher mobility means faster decorrelation of the

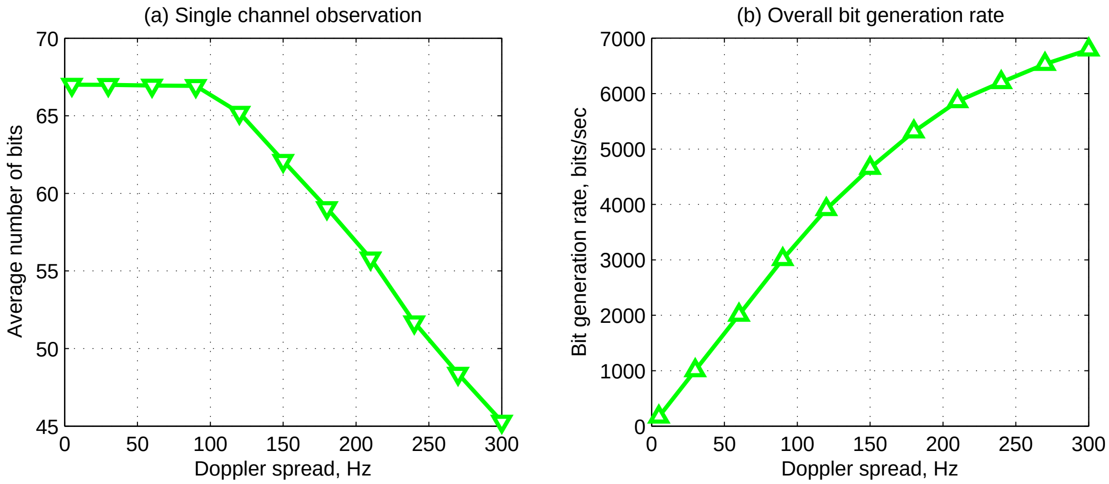


Figure 4.11: Average number of secret bits generated from a single channel observation (a), and overall secret bit extraction rate (b), as a function of the Doppler spread (250μs delay), SNR=30dB, N=64, Enhanced 3-way PS mechanism.

channel. On one hand, this signifies a lower average number of bits generated from a single channel observation due to the decorrelation problem discussed above. On the other hand, this means a faster observation of an uncorrelated channel, i.e. faster re-use of the channel to extract secret bits. Actually, it has been found that the channel decorrelates completely after an interval approximately greater than: $\frac{2}{f_D}$. Therefore, after this interval it is possible to get new independent channel estimates and apply the key generation mechanism to obtain a new set of secret bits.

In Fig. 4.11(b), the secret key extraction rate in sbits/sec as a function of the Doppler spread is plotted. We observe that the secret bits extraction rate increases as a function of mobility. In particular, it increases from 167.5 sbits/sec to 6793 sbits/sec for an increase of the maximum Doppler frequency from 5 Hz to 300 Hz. We can deduce from this graph that mobility is an advantage to the key generation procedure as it permits a higher secret bits extraction rate.

In conclusion, we can say that key generation from multipath channels is particularly interesting in mobile scenarios where the continuous variation of the channel can be leveraged to derive longer and faster keys. Moreover, it can be argued that key generation mechanisms from wireless channels might not be secure in static scenarios and might be vulnerable to dictionary attacks. An attacker can obtain offline measurements of the channel in different locations and use the location information to guess the derived key. However, the success of such an attack is restricted with the non-variation of the channel. This means that there is no mobility of any reflecting cluster and that all parameters that affect the radio propagation (e.g. temperature, humidity) are constant. However, this might not be possible in real scenarios.

4.5 Reconciliation and Key Verification

4.5.1 Reconciliation

Reconciliation refers to the process of error correction in order to remove any discrepancies between the derived keys. It is mainly based on exchanging parity check bits or syndromes between the two nodes, and the application of an Error Correcting Code (ECC). Yet, the price of such an exchange is the loss of some secrecy. As a result, a smaller key is obtained.

Based on a reliability-efficiency tradeoff, ECCs with different rates can be used. While a more powerful ECC leads to a more reliable error correction, a less powerful ECC has the benefit of a lower secrecy loss. Moreover, ECCs of different block sizes can be used. However, the block size of an ECC is restricted to the size of the derived key. Therefore, using ECCs of long block sizes might not be always possible in the case of secret key reconciliation.

In this section, we investigate the application of error correcting codes of different key sizes. We consider the case of a key size in the order of 128 bits and the case of a longer key in the order of 1024 bits. We discuss the efficiency of applying the error correcting code in conjunction with higher quantization in comparison to lower level quantization.

4.5.1.1 Case of a short key

In some scenarios, only a short key can be derived. Consequently, only a small block size ECC can be applied for the purpose of key reconciliation. In this section, we consider a key size in the order of 128 bits and investigate applying a BCH(127,106) code. We compare the results to a 1-bit lower level quantization which corresponds to a decrease of the key size from 126 to 105 bits.

In Fig. 4.12, we plot the probability of error as a function of the quantization precision for a TNR of 36dB. We observe that the probability of error drops down in a dramatic way as the quantization precision drops down from 6 to 5 secret bits.

We compare the lower quantization approach to the BCH(127,106) approach in Fig. 4.13. We observe that while applying a BCH code leads to some performance improvement, the lower quantization approach shows a considerably better performance. This is mainly due to the fact that using the BCH(127,106) ECC helps in correcting up to 3 bit errors while using a 1-bit lower quantization decreases dramatically the bit error rate as we can see in Fig. 4.12. Hence, we conclude that in case of relatively

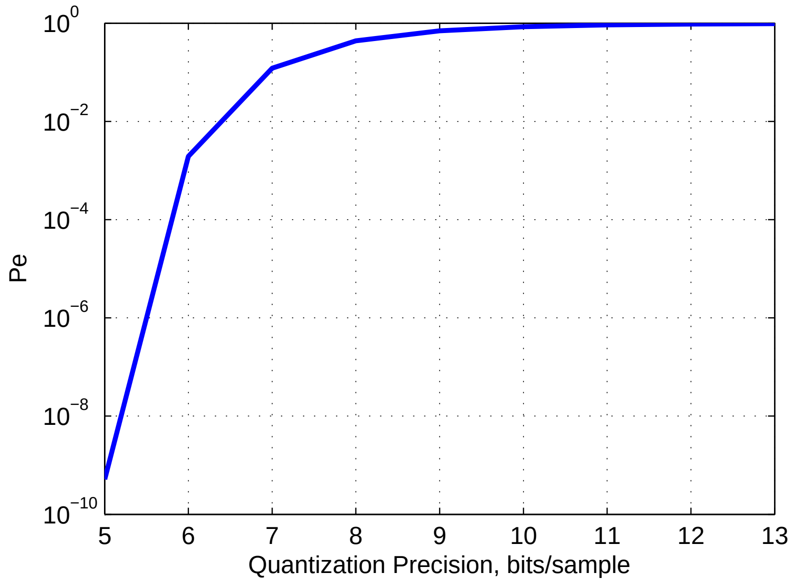


Figure 4.12: Probability of error as a function of the quantization precision for a TNR=36dB, PS mechanism.

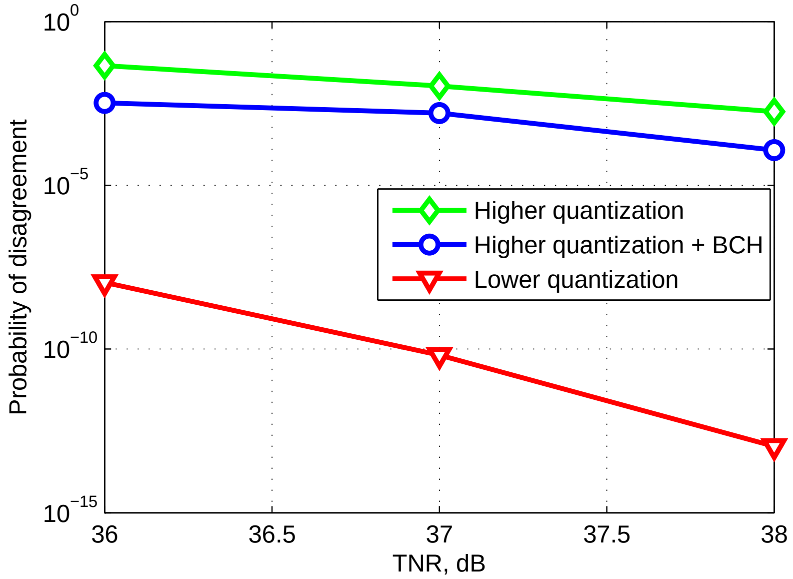


Figure 4.13: Probability of disagreement as a function of TNR for the two approaches.

small key sizes, the application of an error correcting code might not be very useful for improving the reliability of the key generation process.

4.5.1.2 Case of a longer key

The extraction of longer keys allows the employment of more powerful error correcting codes, and hence stronger error correction. In fact, most powerful ECCs require a sufficient block size in order to provide a powerful error correction. For example, LDPC codes are known for their powerful error correction capability approaching the theoretical bounds for a block size larger than 500 bits.

In the previous sections, we have seen that the extraction of such key sizes is indeed possible in wireless networks. Though a single channel realization allows the extraction of about a hundred bits only, this number would be multiplied by using multi-antennas. Moreover, we have seen in Section 4.4.4 that longer keys can be extracted by leveraging the varying nature of the wireless channel due to mobility. Hence, by accumulating secret bits over time, a key of reasonable size can be extracted.

In this section, we show the effectiveness of adding a reconciliation stage based on LDPC error correction to the key generation procedure. We consider a target probability of error[2] less than 10^{-5} and we compare, in terms of key extraction rate, the application of LDPC error correction with higher quantization precision to the case of lower quantization precision without any error correction.

We assume that about 1000 secret bits can be extracted and hence available for reconciliation in case of a higher quantization precision, whereas a lower number is available in case of a lower quantization precision. We apply an LDPC error correcting code based on the secure sketch method described in Section 4.1.2. In this case, the reconciliation stage includes the exchange of LLRs (Log Likelihood Ratios) over the public insecure channel.

To achieve a higher key generation rate, we consider an adaptive LDPC decoder where the code rate varies according to the received SNR in order to achieve the highest efficiency at a low probability of error. The parameters (code rate (R) and number of quantization levels (M)) of the adaptive quantization and LDPC decoding are summarized in table 4.1.

Table 4.1: Adaptive LDPC decoding parameters

SNR	0	1	2	3	4	6	7	9	11	13	14	16	18	24	30	36	42
M	2	2	2	2	4	4	4	8	8	8	8	16	16	32	64	128	256
R	1/6	1/4	1/3	1/2	1/3	1/2	2/3	1/2	2/3	3/4	4/5	2/3	3/4	4/5	5/6	6/7	7/8

[2] Usually, 10^{-5} is considered as an infinitesimally low probability of error

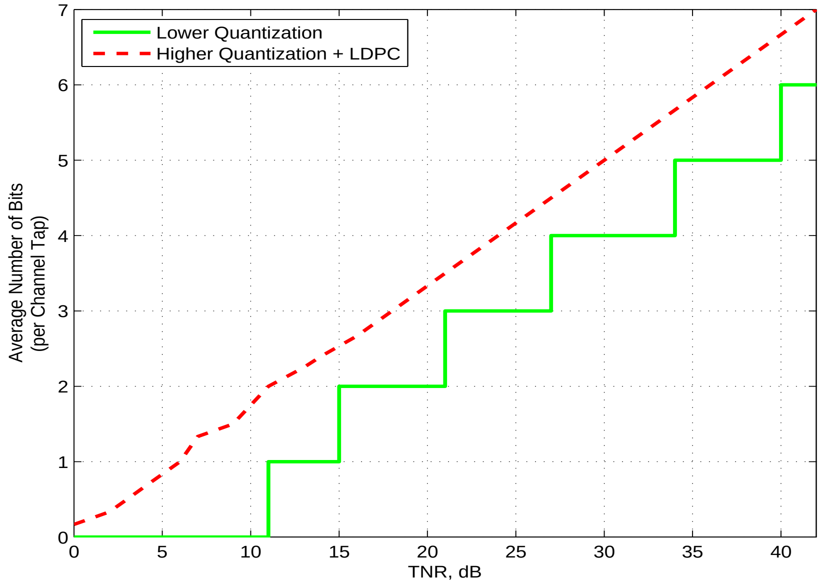


Figure 4.14: Comparison of the average number of bits generated with and without LDPC decoding.

In Fig. 4.14, we compare the average number of bits generated per channel tap as a function of the TNR. We observe that using a powerful LDPC error correcting code can indeed enhance the key generation rate considerably. This enhancement can be clearly observed at low SNRs where the absence of an ECC leads to a zero secret bit extraction rate. In conclusion, we deduce that applying a powerful error correcting code can improve the efficiency of a key extraction mechanism, mainly at low SNRs where error correction is essential to obtain a positive key generation rate.

4.5.2 Key Verification

Key verification is the last step of the key generation process. The purpose of this step is to verify that the two nodes have indeed acquired the same key. One of the possible ways to achieve this goal is exchanging a hash value of the key. However, the exchange of the hash value over the public insecure channel decreases the entropy of the key. In fact, the security of the derived key depends directly in this case on the security of the hash function.

Another common way to achieve key verification is by sending an encrypted nonce. In this case, one of the nodes encrypts a common nonce and transmits it to the other node. Thus, the other node, already knowing the nonce, verifies if the key used to encrypt the nonce is the same as the one in its possession.

4.6 Summary

In this chapter, we have investigated key generation on the physical layer based on the wireless multipath channel. We first reviewed some of the related work and background on this topic. After that, we presented our proposed intelligent mechanisms for shared-key generation based on mitigating error in the quantization of the channel taps either through guard intervals (GI method) or by shifting the phases of the channel taps synchronously (PS method). By deriving the optimal quantization parameters as a function of SNR, we showed that a high efficiency of secret key extraction can be achieved. We also discussed the possibilities of further enhancements by averaging over multiple OFDM symbols and using higher FFT sizes. Through simulations, the proposed PS mechanism was shown to provide a high efficiency of secret bits extraction with more than 90 bits extracted per single channel realization in a typical SISO outdoor channel model.

In addition to that, we have investigated some practical issues that might affect the performance and reliability of key generation from the multipath wireless channel. Mainly, we have investigated the effects of delay between the channel estimates and mobility on the performance and we have showed that our Enhanced 3-way PS mechanism can indeed mitigate the effects of delay and mobility. The 3-way handshake procedure allows to model and correct the slight channel variation due to delay. Whereas, channel variation at higher mobility can be mitigated by modeling this variation as an added error and optimizing the quantization parameters accordingly.

The established Enhanced 3-Way PS mechanism resulted in a decreasing average number of secret bits generated from a "single" channel observation as a function of the Doppler spread. Yet, it was proved that mobility is in fact an advantage to the key generation procedure due to the faster decorrelation of the channel permitting a faster re-keying. The results obtained through simulations showed that the overall secret key extraction rate increases as a function of mobility despite the lower average number of secret bits extracted per a single channel realization.

In the last section, we have investigated reconciliation through error correcting codes and key agreement which form the last stage of a key generation procedure. It has been shown that by applying an appropriate error correcting code, the key generation efficiency can be further enhanced, especially at low SNRs.

As for future work, we will investigate applying more efficient encoding techniques like joint encoding. It would be also very interesting to consider synchronization and frequency offset issues and test our proposed algorithms through real implementations and investigate key refreshment rates in real scenarios.

Chapter 5

Advanced and Secure Medium Access

Contents

Wireless networks have rapidly gained popularity for many reasons, mainly mobility support, simplicity, and fast installation speed. However, the broadcast nature of wireless communication poses many problems related to access control and distribution of resources. IEEE 802.11 [10] is the *de facto* standard for Wireless Local Area Networks (WLANs). It specifies both the Medium Access Control (MAC) layer and the Physical layer of WLANs. The basic medium access control scheme defined is the Distributed Coordination Function (DCF)[1]. It is a distributed contention resolution scheme and

[1] The IEEE 802.11 standard proposes another access method called Point Coordination Function (PCF). However, this mode is optional and very few APs actually implement it. Moreover, the 802.11e

uses the *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) mechanism.

Many security protocols such as WEP, WPA, and WPA2 provide authentication schemes to control the accessibility to the network and the provided services. Yet, these protocols do not provide adequate means to maintain a fair access to the wireless medium and a fair distribution of resources on the different users. The proposed medium access technique assumes a cooperative behavior of all participating hosts to ensure a reasonably fair throughput distribution. Hence, it is very vulnerable to manipulating and cheating selfish nodes. A malicious node that does not adhere to the network access protocol can easily obtain an unfair share of the common wireless channel or disrupt the normal operation of the network. Indeed, it has been found that the presence of malicious nodes that deviate from the DCF contention resolution scheme can reduce dramatically the throughput share received by the well behaving nodes [11, 12, 13]. Furthermore, the impact of MAC layer misbehavior can reach the level of a Denial-of-Service (DoS) attack. Therefore, the development of mechanisms for detecting misbehavior and ensuring a fair channel contention is very essential in WLANs.

While some proposed solutions have considered misbehavior detection on the MAC layer, many proposals have targeted establishing more advanced and secure medium access schemes. Indeed, being a contention-based medium access scheme, DCF is not only vulnerable to misbehavior but also suffers from a high collision rate which leads to a suboptimal use of bandwidth.

In this Chapter, we first review the basic access scheme used in IEEE 802.11 networks and we highlight its vulnerability to misbehavior and its bandwidth efficiency. We mainly focus on backoff misbehavior and show how it may lead to an unfair share of the wireless channel. We review some of the related work on this topic and propose the Random Backoff Control (RBC) mechanism that allows MAC layer misbehavior detection and mitigation. This mechanism provides a countermeasure against MAC layer DoS attacks and ensures a fairer distribution of network resources. The second part of this chapter is concerned with advanced and secure medium access schemes. In this part, a review of some of the related work on this topic is first given. After that, we describe our proposed Self-Organized Distributed Channel Access (SODCA) scheme. Distinctively from all proposed solutions, our novel medium access scheme is a distributed, efficient, secure and dynamic scheduling scheme. Nevertheless, it does not incur any additional overhead. Finally, the efficiency of SODCA is manifested through

amendment proposed the Enhanced Distributed Channel Access (EDCA) which is an enhancement to DCF that supports quality of service. Yet, the analysis and results in this dissertation can be easily extended to EDCA. Therefore, we base our analysis on DCF as being the fundamental channel access technique in wireless IEEE 802.11 networks.

extensive simulations based on the OMNeT++ network simulator.

5.1 Overview of the MAC layer

5.1.1 The Distributed Coordination Function (DCF)

DCF is the main contention and medium access technique used in IEEE 802.11 systems. It combines the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism with a Request to Send / Clear to Send (RTS/CTS) handshake mechanism to avoid collisions, avoid the hidden terminal problem [92], and to provide a distributed access to the channel.

The CSMA/CA with RTS/CTS handshake mechanism works as follows. When a node has a packet to transmit, it checks the status of the channel before transmitting data. It applies CSMA sensing by using physical and virtual carrier sensing mechanisms. The physical carrier sensing mechanism is known as Clear Channel Assessment (CCA) which is a physical measurement taken by the radio interface that determines if the wireless medium is busy or not. Whereas the virtual carrier sensing mechanism is achieved on the MAC layer by reading the duration values in the headers of the MAC layer control packets which inform other stations about the duration of a transmission. When the channel is sensed both physically and virtually as idle for a period of time greater or equal to a Distributed Inter Frame Space (DIFS), the packet transmission may begin at the beginning of the following time slot. Yet, to avoid collisions, a random backoff mechanism is employed such that a node backoffs for a certain random period chosen randomly in the interval $[0, CW-1]$ where CW is the Contention Window size. The backoff counter is then decremented for every idle time slot until reaching zero. Consequently, the node transmits an RTS packet to the destination which replies with a CTS packet after waiting for a Short InterFrame Space (SIFS). The transmission of the CTS packet ensures that all nodes in the radio range of the receiver will defer their transmission. The data frame is then transmitted and the receiver responds with an acknowledgment (ACK). This procedure is illustrated in Fig. 5.1.

This handshake ensures that all nodes in the neighborhood of the transmitting node and the receiving node overhear the current transmission, and hence avoid the hidden terminal problem. They defer then their own transmission to a NAV (Network Allocation Vector) period obtained from the duration field in the RTS, CTS or Data packets and which is calculated as:

$$NAV(RTS) = 3 \times SIFS + T_{CTS} + T_{DATA} + T_{ACK} \tag{5.1}$$

$$NAV(CTS) = 2 \times SIFS + T_{DATA} + T_{ACK} \tag{5.2}$$

$$NAV(DATA) = SIFS + T_{ACK} \tag{5.3}$$

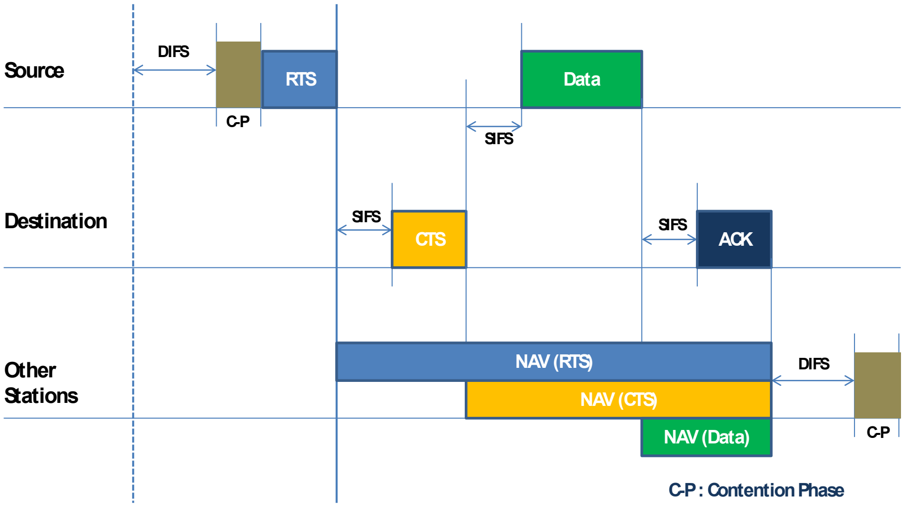
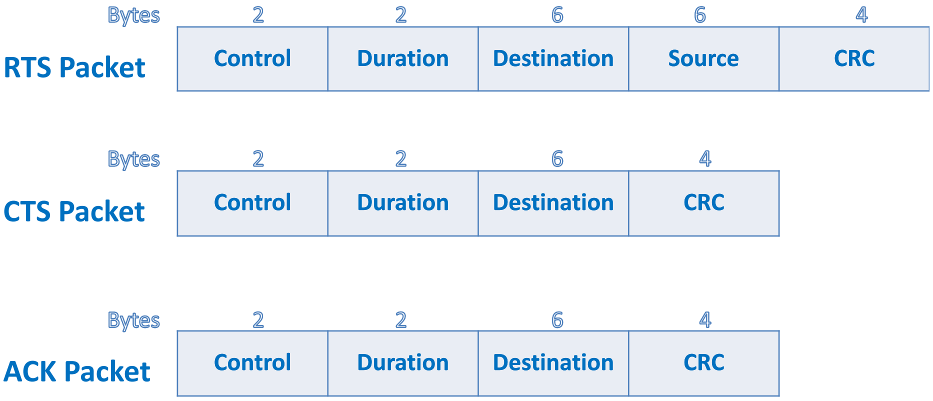


Figure 5.1: IEEE 802.11 DCF channel access technique.



RTS Packet

Bytes	2	2	6	6	4
RTS Packet	Control	Duration	Destination	Source	CRC

CTS Packet

Bytes	2	2	6	4
CTS Packet	Control	Duration	Destination	CRC

ACK Packet

Bytes	2	2	6	4
ACK Packet	Control	Duration	Destination	CRC

Figure 5.2: IEEE 802.11 MAC layer control packets format.

However, the transmission of an RTS packet does not always lead to a successful contention on the channel. Indeed, two different nodes might transmit two RTS packets in the same time slot which leads to a collision. Therefore, the DCF scheme implements additionally a Binary Exponential Backoff (BEB) mechanism to decrease the probability of collision in case of congestion. BEB requires transmitting nodes to double their contention window size in case of a collision up to a maximum value

$CW_{max} = 1024$ and reset the contention window to the default value $CW_{min} = 32$ in case of a successful transmission.

5.1.2 Vulnerabilities of DCF

Many recent works [11, 12, 13, 93, 94, 95, 96, 97, 98] have showed that the current IEEE 802.11 systems are vulnerable to MAC layer misbehavior, either due to the control packets format or due to the DCF technique. In fact, the DCF technique defined for the MAC layer of IEEE 802.11 systems does not provide any control of the channel access and requires a cooperative behavior of all participating nodes. Hence, it is very vulnerable to misbehavior or malicious attacks[2]. Malicious behavior is even more facilitated through the RTS/CTS handshake mechanism. Indeed, many attacks have been discovered that target the access scheme of the MAC layer in IEEE 802.11 systems. In this section, we describe briefly some of the most powerful attacking strategies on the MAC layer in WLANs.

5.1.2.1 Backoff Manipulation Attack

In order to ensure a fair access to the channel, DCF assumes that all nodes obey the contention mechanism and choose a backoff value randomly in the interval $[0, CW - 1]$. However, a misbehaving node can simply always choose a small backoff value.

Let us consider for example the widely used naive attacker model. It is a generic attacker model that is normally used to inspect the resilience of a MAC layer access scheme to different levels of misbehavior. Basically, a naive attacker chooses a random backoff in the interval $[0, \gamma * (CW - 1)]$ where $(1 - \gamma)$ is the misbehaving coefficient. The effect of such a misbehavior is shown in Fig. 5.3 for a network of 6 nodes where 1 is misbehaving (see Section 5.2.3.1 for simulation parameters). We can observe that as the misbehaving coefficient increases, the throughput of the attacker (or misbehaving node) increases whereas the throughput of a well behaving node decreases dramatically.

We define also an aggressive attacker as an attacker who is in acquaintance of all protocol parameters, and who uses the optimal strategy to get the maximum share of the channel. In the case of DCF, the aggressive strategy consists of choosing always a zero backoff value. This corresponds to a misbehaving node with $(1 - \gamma)$ equal to 1 in Fig. 5.3. In this case, we observe that the attacker gets full access to the channel while the legitimate nodes are under a Denial-of-Service attack.

Considering its serious impact, we investigate in this dissertation mechanisms to thwart or avoid this kind of MAC layer misbehavior.

[2] We do not differentiate, in this thesis, between a malicious node (attacker) who targets disrupting the communication and a selfish node applying the same technique but for the purpose of getting a higher share of the channel.

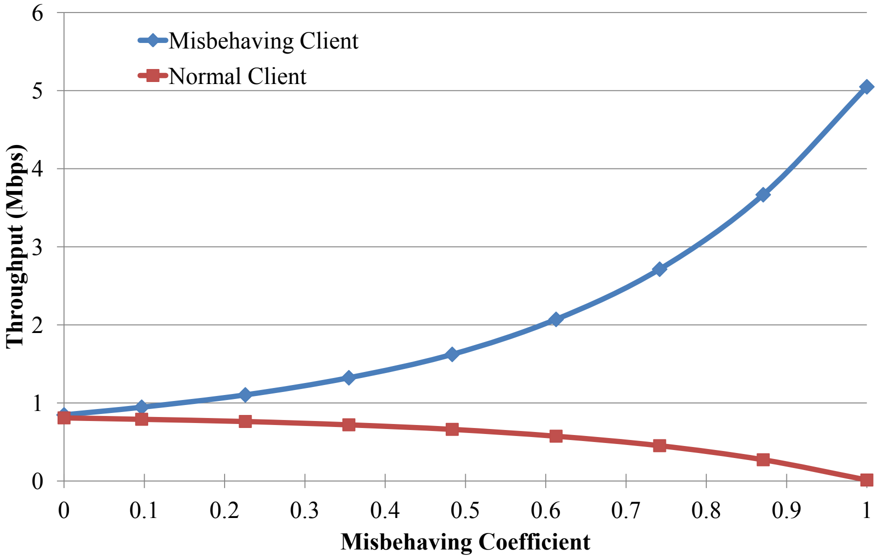


Figure 5.3: Impact of misbehaving on the throughput distribution.

5.1.2.2 Shorter DIFS/EIFS

The DCF scheme requires each node to physically sense the radio channel for a duration of DIFS before entering in the backoff state. However, a selfish node can simply manipulate these parameters and wait for a shorter DIFS to get a more prioritized access to the channel. The DOMINO framework [94] proposes a simple test based on monitoring the idle period after each ACK and detecting any station that is transmitting before the required DIFS period. However, such a solution requires high level synchronization.

Moreover, the DCF scheme requires each node to defer for a duration equal to the Extended Inter-Frame Space (EIFS) in case of a sensed collision or an undecodable packet. Yet, a selfish node can also choose to defer for a shorter period. This can be also detected by a similar detection test.

5.1.2.3 Duration Inflation Attack

Control frames such as RTS, CTS and ACK frames carry a duration field which informs about the duration of a data frame transmission. This field is 16 bits long and has a maximum value of $32767\mu s$. Nodes overhearing any of these control frames defer their transmission for a time period equal to the value of this duration. An attacker can set a large duration value in the RTS frame and hence reserve the channel to the maximum allowed duration even when sending a short data frame or without sending any data at all[3]. By doing so, all stations receiving these frames will set their NAV value to the maximum set value, and enter a deferring state. This type of virtual jamming attacks is called duration inflation attack or oversized NAV [94, 98]. Detecting this kind of attack can be performed simply at the AP by comparing the actual duration of a transmission and comparing it with the NAV value in the RTS and DATA frame headers as proposed in the DOMINO detection system [94].

5.1.2.4 Jamming Attack

Jamming has always been considered as a serious problem on the physical layer of wireless communications. Yet, this attack is further facilitated by the RTS/CTS handshake mechanism of the MAC layer. In this case, an attacker does not need to continuously jam the wireless spectrum and deplete its power. It only needs to jam the control frames of the RTS/CTS handshake mechanism to disrupt the network. The most effective way to perform such an attack is to jam the ACK packets.

In fact, all data packets need to be acknowledged on the MAC layer before being cleared from the transmission queue. The attacker can calculate easily the exact time of sending the ACK frame by subtracting the SIFS value from the NAV(DATA). When the ACK packet is successfully jammed, the sender has to reschedule the data transmission even though the data has been correctly received by the receiver. This attack called the Jamming ACK (JACK) attack [99], can be used by malicious nodes to drain the battery energy of victim nodes.

Since mitigating such an attack, as any jamming attack, requires methods for detection of the sources of jamming and isolation of the jamming node, we do not consider this type of attack in this dissertation.

5.1.2.5 Virtual Jamming Based on False CTS/ACK

The authors in [92] investigated some other hidden vulnerabilities in the control packets format. They pointed out that CTS and ACK packets do not include the address of the sender or any other authentication scheme, as we can observe in Fig. 5.2. The main reason behind this is the optimization of the packets' sizes. However, this enables a malicious node to perform virtual jamming on the neighboring nodes using false CTS or ACK packets.

The authors propose cryptographic and non-cryptographic solutions to tackle this problem. The main idea to thwart this kind of attack is authenticating the CTS and ACK packets, and ensuring their integrity as proposed in [92].

[3] This refers to virtual jamming based on false-RTS packets

5.1.3 Efficiency of DCF

Scheduling-based techniques as TDMA (Time Division Multiple Access) offer a high bandwidth efficiency. However, it is difficult to perform scheduling between different terminals with different traffic rates and applications. Hence, contention based techniques have attracted more attention in wireless networks. This has lead to the wide adoption of the DCF channel access technique.

Although DCF is a distributed channel access technique, its design achieves a high bandwidth efficiency. Indeed, the different mechanisms implemented in the DCF decrease dramatically the number of collisions. The RTS/CTS handshake mechanism solves the hidden terminal problem [92] and helps in avoiding collisions between long data packets. And the BEB mechanism helps in lowering the probability of collision in case of congestion.

Yet, the DCF technique is not optimal. It suffers from a decreasing total throughput as the congestion state increases, as we can observe in Fig. 5.4. The total network throughput decreases as the total number of active nodes increases. Moreover, the contention phase leads to a sub-optimal use of bandwidth mainly in the case of large backoff values.

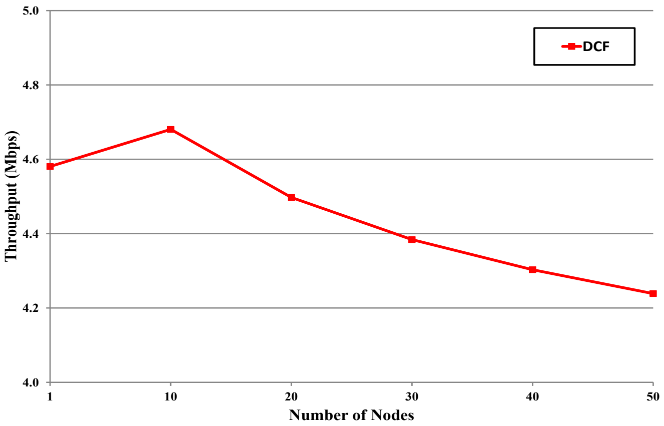


Figure 5.4: Total throughput as a function of the number of nodes, DCF.

5.2 Thwarting Misbehavior on the MAC Layer

We have seen in the previous discussion that the DCF scheme is vulnerable to backoff manipulation. The main reason behind that is the assumption of a cooperative behavior of the wireless nodes and the absence of control of the backoff values. Hence, any wireless node can easily get a higher share of the channel by choosing smaller backoff values. While some works have proposed probabilistic misbehavior detection mechanisms, we propose in this section a deterministic misbehavior detection mechanism. It is based on minor modifications to the contention resolution mechanism in the DCF scheme through the Random Backoff Control (RBC) mechanism. Before describing RBC, let us first review some of the related work on this subject.

5.2.1 Related Work

There is a vast literature on MAC layer attacks and countermeasures. References [11, 12, 93] summarize some of the main attacks that can be carried out on the MAC layer in IEEE 802.11 systems. On the other hand, there are many works that tackle the problem of misbehavior on the MAC layer in WLANs and provide more resilient access schemes and misbehavior detection mechanisms.

In [96], a centralized approach was proposed to tackle the problem of backoff manipulation. In this approach, the Access Point (AP) is associated the task of assigning backoff values to the nodes. Consequently, a detection mechanism can be employed based on monitoring the difference, over a certain number of frames, between the chosen backoff values of a node and those associated by the AP. This method has been proven to be capable of detecting misbehaving nodes efficiently. However, it lacks the advantages of a distributed mechanism and it requires severe modifications to the MAC protocol. Extensions of this approach to Ad Hoc networks have also been proposed in [100, 101].

Jaggi et al. have proposed a distributed detection and reaction mechanism to thwart misbehavior in [102, 103]. In their approach, each node is supposed to measure its throughput over a certain cycle. In case a node detects a misbehavior (by observing that its throughput is 80% or less of its expected throughput), it applies a reaction mechanism to increase its throughput by fixing a smaller contention window and a time window over which the reaction mechanism is to be applied. The authors perform simulations in NS2 and prove that the throughput of the nodes would then converge to a uniform value. Moreover, it is shown that such a reactive approach leads to a lower total throughput in case of misbehavior and hence forces the adversary to cooperate as this becomes its optimal strategy. In fact, it has been proven through game theory, in [104], that the optimal strategy in case of multiple adversaries or reacting nodes is cooperation. Otherwise, a small proportion of selfish or non-cooperative nodes can lead to a network collapse.

Venkatarama et al. [105] have proposed a wired-side approach to detect MAC layer misbehavior. Their approach is based on monitoring the packets inter-arrival time (IAT) and detecting any abnormality or deviation from the normal distribution. The authors have considered different attacks such as CW manipulation and DIFS manipulation and they have shown the impact of these attacks on the distribution of the IAT. Consequently, they have proposed using a naive Bayes classifier to compare IAT profiles and detect any misbehavior. Simulations and experiments were performed to validate the proposed scheme.

Raya et al. [94, 106] have proposed a detection system called DOMINO that does not require any modifications to the MAC protocol. The detection system is based on performing several tests to detect the different types of misbehavior (backoff manipulation, oversized NAV, shorter than DIFS). The detection system is implemented at the AP which collects periodically the traffic traces of all the users and runs the different tests. Each of these tests corresponds to a designated misbehavior. Hence, the aggregated results of these tests infer whether a certain node is misbehaving or not. To detect the backoff manipulation attack, the authors propose 3 tests. The first one is based on calculating a maximum backoff over a set of samples and comparing it to a certain threshold. Yet, this test can be easily tricked by a malicious node as discussed by the authors. The second test is based on calculating the average backoff of a certain node and comparing it to a nominal average backoff value. To lower the false positive rate, the authors propose an additional confidence parameter. They also propose detection after suspicion for k-times. However, this reduces the responsiveness of the system and makes it vulnerable to short term or adaptive[4] misbehavior as discussed in [101]. Finally, the authors also propose another test to tackle the problem of upper layers delay. It is based on calculating the average of consecutive backoff values and comparing it to a nominal value.

It is important to note that these tests are probabilistic tests and non-deterministic. This means that they can offer detection up to a certain confidence interval but suffer from a non-vanishing false positive rate. Hence, there is a trade-off between the false positive rate and the misbehavior detection performance.

The DOMINO system was further investigated by Cardenas et al. in [107, 108]. The performance of DOMINO has been analyzed and it was shown that a cumulative sum detection mechanism outperforms the average backoff detection mechanism implemented in DOMINO. Moreover, both mechanisms were compared to a detection mechanism based on the Sequential Probability Ratio Test (SPRT) [109]. Simulation results have shown that SPRT outperforms both mechanisms. Yet, it is important to note that SPRT is a parametric statistic. This means that it requires exact models of the normal and adversarial distributions. On the other hand, DOMINO and the proposed extensions are non-parametric and require only some nominal knowledge.

Guang et al. have proposed a misbehavior detection mechanism, called Predictable Random Backoff (PRB) in [97]. PRB is based on modifying the random backoff mech-

[4] The authors argue that the cheater does not know the detection and monitoring parameters to adapt its behavior. Evidently, this is not a secure assumption.

anism of the DCF protocol to make the random backoff predictable up to a certain interval by lower bounding the contention window. Hence, if the selfish node does not follow PRB and chooses a backoff value smaller than the predictable lower bound, the receiver (or AP) can easily detect the misbehavior. This algorithm was further presented in an analytical model in [11]. Both simulations and analysis show that PRB can effectively diminish the impact of backoff misbehavior.

5.2.2 The Random Backoff Control Mechanism

The key idea of the RBC mechanism is to control and limit the backoff selection procedure in order to enable a deterministic detection of backoff manipulation and ensure a fair access to the channel. In RBC, the bounds on the backoff value of a node vary according to its previous backoff value in order to prevent backoff manipulation. For example, a node is forced to choose a larger backoff value in the next transmission whenever it chooses a relatively small backoff value.

To accomplish this goal, we propose to lower bound the contention interval with a contention window lower bound CW_{lb} which changes according to the behavior of the node, as suggested in the PRB mechanism proposed in [97]. However, the contention window lower bound varies in RBC in a way to ensure fairness in channel access. In the following, we first summarize briefly the PRB algorithm and then we describe the RBC algorithm and show how it ensures a fairer channel access even in the presence of aggressive selfish nodes.

5.2.2.1 Overview of PRB

The Predictable Random Backoff (PRB) mechanism [97] allows to predict up to some extent the backoff values chosen by the participating nodes. Its main idea is to lower bound the contention interval with a contention window lower bound CW_{lb} which changes according to the behavior of the node. Any node that does not adhere to PRB is then detected as a misbehaving node and penalized. Hence, a selfish node has to adhere to the PRB mechanism to avoid being detected. As a result, the negative impact of misbehavior on the network performance is reduced.

In *Algorithm 1*, we show the main algorithm of PRB. Initially, CW_{lb} is set to zero and hence a node with a data packet to transmit chooses a backoff value randomly in the interval $[0, CW-1]$. Upon every successful data transmission, a new lower bound of the contention window is computed according to the backoff value b_i. If $\alpha_l \times b_i$ is less than a certain threshold CW_{thresh}, the lower bound for the next contention window is computed as $CW_{lb} = \alpha_l \times b_i$. In case b_i is selected as 0, CW_{lb} is set to a specified value CW_{lb}^{spec}. Otherwise, CW_{lb} is set to a default value equal to 0. Therefore, the node has to select a backoff value from the interval $[CW_{lb}, CW-1]$ in the next contention period. Otherwise, it would be detected as a misbehaving node.

Algorithm 1 Predictable Random Backoff

```
$CW_{lb} = 0$
$b_0 \leftarrow [CW_{lb}, CW - 1]$
for each sending packet $P_{i+1}$ do
    if $\alpha_l \times b_i < CW_{thresh}$ then
        if $b_i == 0$ then
            $CW_{lb} = CW_{lb}^{spec}$
        else
            $CW_{lb} = \alpha_l \times b_i$
    else
        $CW_{lb} = 0$
    $b_{i+1} \leftarrow [CW_{lb}, CW - 1]$
```

As we have seen above, the key idea of PRB is to force the node that chooses a small backoff value to choose a larger backoff in the next transmission through the introduced contention window lower bound. Otherwise, the node will be detected as misbehaving. It has been shown in [97] that by following the PRB mechanism, the negative impact of a naive misbehaving node is reduced.

However, in [97], the case of an aggressive and adaptive cheating node has not been considered. In fact, a node can adaptively change its backoff value and achieve a higher throughput while obeying the PRB mechanism. In PRB, the parameters α_l, CW_{thresh} and CW_{lb}^{spec} were set to 2, 31 and 4 respectively. Hence, a smart aggressive node can continuously choose a sequence of backoff values of 0, 4, 8, and 16 without being detected by the PRB mechanism. In this case, this node achieves an average backoff value of 7 which is far from the expected normal value of a well-behaving node which is lower bounded by 16 (most optimistic value which corresponds to the case of no collisions). It is clear that a misbehaving node can then achieve a higher throughput than other nodes while still adhering to the PRB mechanism.

5.2.2.2 The RBC Algorithm

The RBC mechanism works in a similar way to the PRB mechanism. The contention window is similarly bounded by a lower bound. The main difference is only in the computation of the lower bound. In RBC, the lower bound is varied in a way so that a node is forced to choose a larger backoff value in the next transmission depending on how small was the previous chosen backoff value. In fact, RBC adapts the value of the lower bound according to the behavior of the node in a way to ensure an average backoff value close to the nominal average backoff. Consequently, this backoff control mechanism minimizes the impact of misbehavior and ensures a fairer access to the channel.

In *Algorithm 2* below, we illustrate the main concept of the RBC mechanism. It computes upon each transmission a new lower bound of the contention window based on the backoff value of the previous round. The function *ComputeLowerBound*, illustrated in Table 5.1, outputs the appropriate CW_{lb} value according to each backoff value chosen in the previous transmission, so that a fair distribution of the network throughput is guaranteed. Moreover, CW_{lb} is set to 0 in the case of a collision or a failed transmission (i.e. $retry > 0$); and similarly with the BEB mechanism, CW is doubled until it reaches a maximum value CW_{max}. This enables a larger contention window and hence decreases the probability of collisions.

Algorithm 2 Random Backoff Control (RBC)

```
$CW_{lb} = 0$
$b_0 \leftarrow [CW_{lb}, CW - 1]$
for each sending packet $P_{i+1}$ do
  if $retry > 0$ then
    $CW_{lb} = 0$
    $CW = max(CW \times 2, CW_{MAX})$
  else
    $CW_{lb} = ComputeLowerBound(b_i)$
  $b_{i+1} \leftarrow [CW_{lb}, CW - 1]$
```

Table 5.1: ComputeLowerBound function

Input: Backoff value (b_i)	Output: CW_{lb}
$0 \leq b_i < 4$	30
$4 \leq b_i < 8$	26
$8 \leq b_i < 12$	22
$12 \leq b_i < 16$	18
$16 \leq b_i < 20$	14
$20 \leq b_i < 24$	10
$24 \leq b_i < 28$	6
$28 \leq b_i < 32$	2
$32 \leq b_i$	0

In Fig. 5.5, we show a throughput distribution comparison between the contention resolution mechanism in DCF, PRB and RBC in the presence of a smart adaptive cheater (Node 5) applying an aggressive strategy to get the maximum possible throughput. In the case of pure DCF, the selfish node can simply always choose a zero backoff

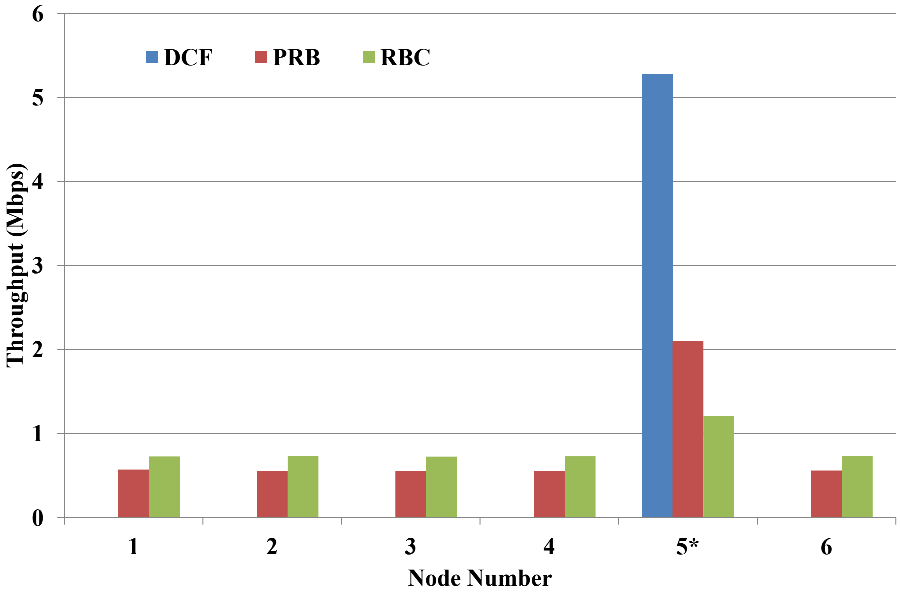


Figure 5.5: Comparison of the throughput distribution of DCF, PRB and RBC over 5 well-behaving and one aggressive misbehaving node (Node 5).

value. We observe from the figure that this strategy allows this node to take full access to the channel. In the case of PRB, the optimal strategy of this selfish node (without being detected) is to choose the backoff values in the sequence (0, 4, 8, 16, 0, ...). Hence, it obtains a higher throughput than any other node. However, we observe that PRB still provides a slightly better throughput distribution. Finally, the optimal strategy of the selfish node in the case of RBC, is to choose a backoff value in the sequence (2, 32, 2, 32, 2, ...). We observe that RBC shows a fairer distribution of the throughput between misbehaving and well-behaving nodes. In the next section, we provide a deeper comparison of these backoff protocols through extensive simulations.

5.2.3 Simulation Results

5.2.3.1 Simulation Setup

Our simulations have been performed using the OMNeT++ network simulator based on the INET framework [110]. The system follows the IEEE 802.11b standard with 11Mbps maximum bit rate, a carrier frequency of 2.4GHz and a maximum transmission power of 20mW. However, similar results are expected for other systems implementing the same contention resolution mechanism as in DCF.

The area size of the simulation topology is equal to $400 \times 400\ m^2$, and all nodes are

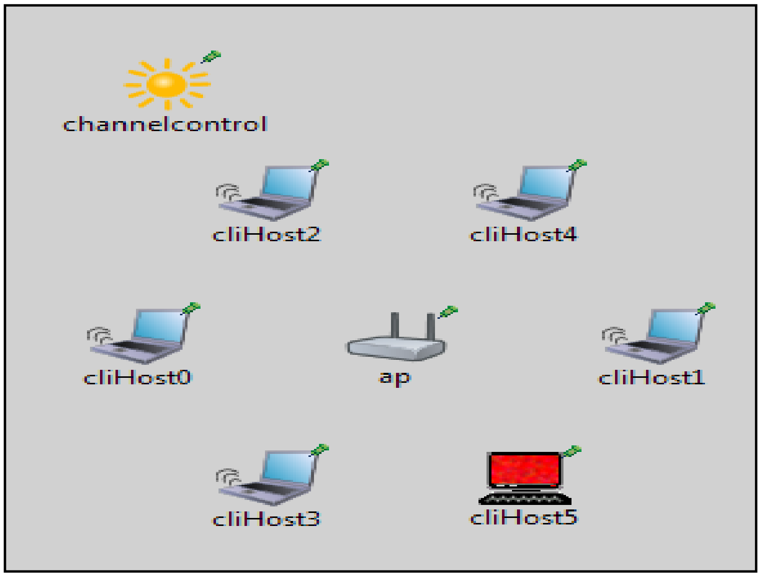


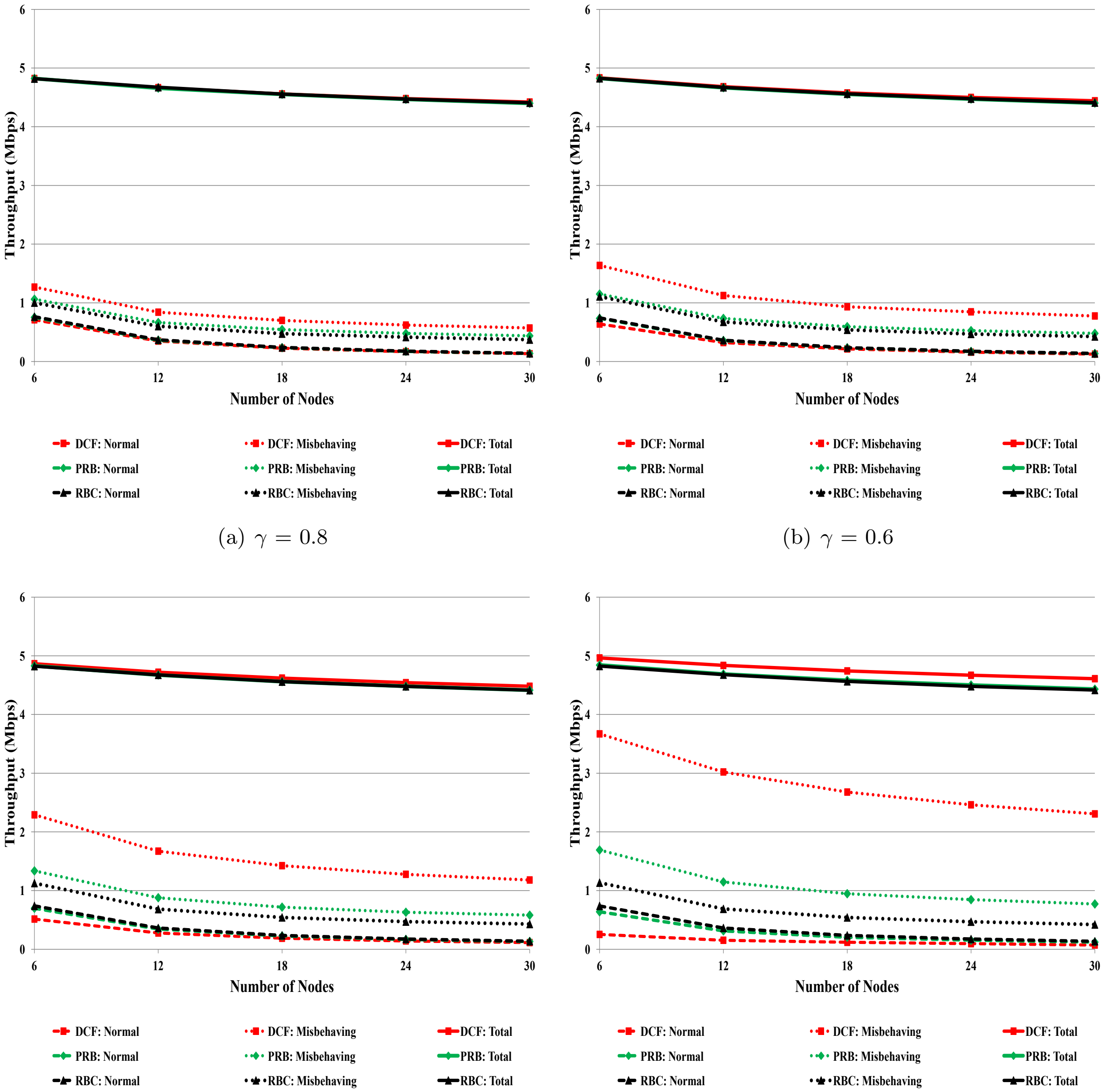
Figure 5.6: Scenario used in the simulations, case of 6 nodes.

located at an equal distance from the access point in order to have a fair comparison of throughput distribution. The traffic type at all nodes is CBR (Constant Bit Rate) of rate $8Mbps$ so that the network is in a congestion state, and the packet size is 1350 Bytes. Moreover, for simplicity and in order to have a fair comparison, we consider a simple path-loss channel model.

We have performed simulations with various number of nodes and measured the total throughput, the throughput of the well-behaving nodes, and the throughput of the misbehaving node in order to compare the contention mechanism in DCF to the PRB and RBC mechanisms. We have run each simulation for a duration of $1000s$. Finally, we note that in all our simulations we have only considered the case of one selfish node that is applying either the aggressive strategy or the naive strategy with a certain misbehavior coefficient.

5.2.3.2 Naive attacker

The naive attacker is a generic attacker model used to study the behavior of a MAC protocol in function of the misbehaving coefficient. In the case of PRB and RBC, a selfish node applying the naive strategy chooses a backoff value from the interval $[CW_{lb}, max(CW_{lb}, \gamma \times (CW - 1))]$ where $(1 - \gamma)$ is the misbehaving coefficient. In the performed simulations, we have considered the γ-values of 0.8, 0.6, 0.4, and 0.2 which correspond to the misbehaving coefficients of 0.2, 0.4, 0.6, and 0.8, respectively.



(a) $\gamma = 0.8$

(b) $\gamma = 0.6$

(c) $\gamma = 0.4$

(d) $\gamma = 0.2$

Figure 5.7: Throughput distribution between normal nodes and a misbehaving node applying the naive strategy.

In Fig. 5.7, we plot the total network throughput as well as the throughput of the well-behaving and misbehaving nodes as a function of the number of nodes for the different values of γ considered, employing pure DCF, PRB, and RBC. We observe that RBC shows a higher resilience to the naive attack since the difference of throughput between a normal node and the misbehaving node is smaller than in the case of PRB. Whereas, DCF shows a poor throughput distribution between the normal nodes and the misbehaving node, mainly at small values of γ. We observe also that there is a slightly lower total network throughput in cases of PRB and RBC. However, if we subtract the throughput of the attacker (misbehaving node) and hence consider the useful network throughput, we obtain a higher total useful throughput using PRB and RBC.

5.2.3.3 Aggressive attacker

As we have mentioned before, an aggressive attacker or misbehaving node has total knowledge of the detection mechanisms employed and hence alternates its backoff values in an adaptive way to evade detection. Since it forms the optimal strategy of a misbehaving node, we study its effect separately on the different mechanisms.

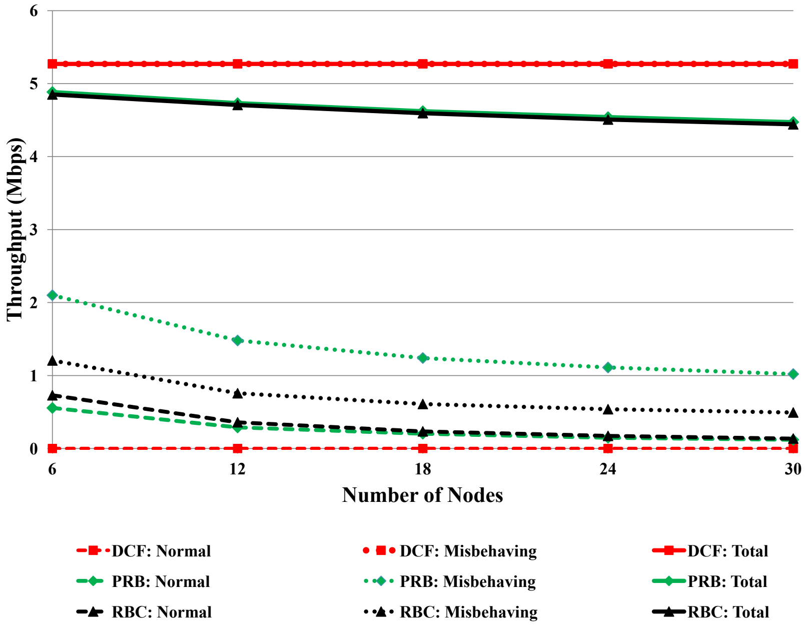


Figure 5.8: Throughput distribution between normal nodes and a misbehaving node applying the aggressive strategy.

In Fig. 5.8, we plot the throughput distribution as a function of the number of nodes employing DCF, PRB and RBC. First, in case of DCF, we observe that the total network throughput is totally consumed by the misbehaving node. Hence, the other nodes are subject to a DoS attack. In case of PRB, we observe that there is a significant difference between the throughput of a well-behaving node and that of a misbehaving node. Whereas, this difference is significantly reduced by using the RBC mechanism. On the other hand, we observe that the RBC mechanism shows a slightly lower total achieved network throughput. However, this decrease is relatively very small and can be considered negligible. If we use the useful network throughput in presence of misbehavior as a comparing parameter, we find out that RBC yields the highest performance.

5.2.3.4 Fairness Index

The Jain's Fairness index [111] is given by:

$$F_J = \frac{(\sum_{i=1}^{N} T_i)^2}{N \sum_{i=1}^{N} T_i^2} \tag{5.4}$$

In Fig. 5.9, we compare the Jain's Fairness index of DCF, PRB and RBC for the naive ($\gamma = 0.2$) and aggressive cases. We observe that RBC outperforms PRB and DCF and achieves a significantly higher fairness index.

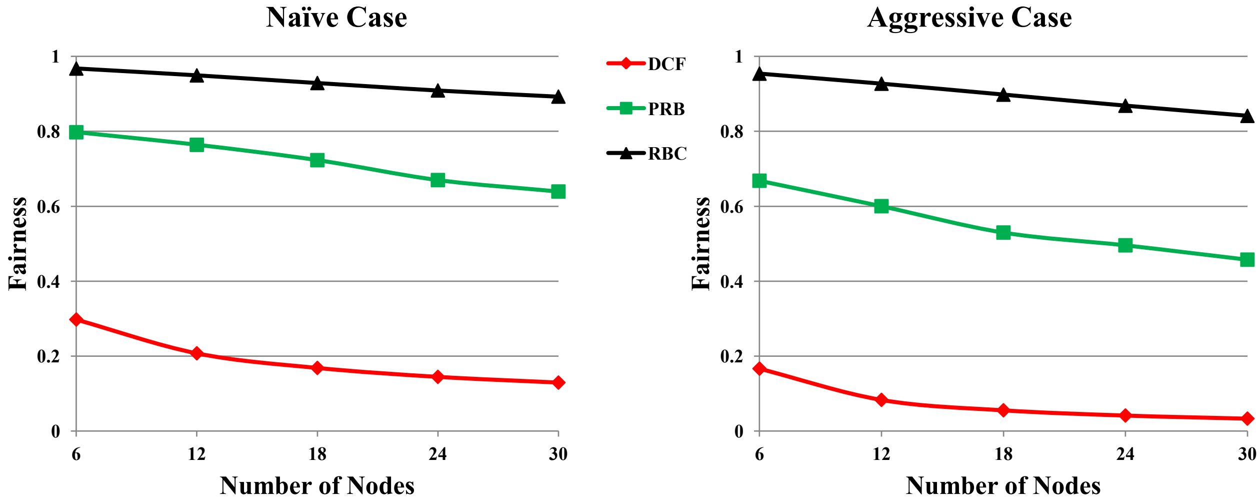


Figure 5.9: Fairness comparison of DCF, PRB and RBC in the case of a naive node ($\gamma = 0.2$) and the case of an aggressive node.

5.2.4 Final Notes

5.2.4.1 Reaction and Misbehavior Prevention

The last step of a misbehavior detection and prevention scheme is ultimately reaction and penalization. Some works [102, 103, 104] have proposed distributed reaction methods to thwart misbehavior and encourage cooperative behavior of all nodes. However, a distributed reaction method tackles only the case of selfish nodes which aim at getting the highest share of the channel. Thus, it facilitates the problem for malicious colluding nodes which aim at disrupting the network operation. Therefore, thwarting misbehavior after detection might require more severe mechanisms. One of the possible mechanisms is disassociation and depriving of network service, for example through not answering RTS packets corresponding to the malicious node or answering with a zero-NAV CTS packet. Hence, the malicious node is deprived of service and from accessing the channel. However, a malicious node can still disrupt the network by sending continuously RTS packets (virtual jamming) or jamming control packets. Hence, a physical intervention by a network administrator might be needed in this case. This might be actually the cost that we have to pay in securing completely a wireless network.

5.2.4.2 Authentication

It is important to note that authentication on the MAC layer is a prerequisite to any MAC layer misbehavior detection mechanism. In the absence of authentication, a malicious node can just simply use multiple identities (a Sybil attack) to escape detection. In addition, an identity theft might ultimately lead to a false positive. Therefore, we assume in our proposed method that an authentication scheme is available. This can be accomplished through physical layer characteristics as discussed in Chapter 4, or based on cryptographic functions as proposed in [93, 95].

5.2.4.3 Implementation

Concerning the implementation, the RBC protocol can be implemented as a firmware update at both the access point and the wireless nodes without the necessity of modifying the formats of the MAC layer packets. In fact, the computation of the contention window lower bound can be performed separately at the access point and the wireless devices without requiring any exchange of parameters. Therefore, we can say that the RBC protocol can provide a detection mechanism of misbehavior and can guarantee a fairer distribution of resources at a negligible cost.

5.2.4.4 Multiple Attackers

We have considered in our study the case of one selfish node (or malicious node). Yet, it is interesting to see the effect of multiple attackers on the distribution of the network throughput. In this case, each selfish node has to consider the strategies of the other selfish nodes to derive its optimal strategy. Interestingly, the aggressive strategy presented in this chapter would not be the optimal strategy in this case since it would lead to a high probability of collision between the selfish nodes and hence a network collapse. In fact, deriving the optimal strategy of a misbehaving node would be then more complicated but could be solved through Game theory.

5.2.4.5 Efficiency

Finally, it is important to note that the above mechanisms offer only a suboptimal bandwidth efficiency. In fact, we observe clearly the decrease of the total network throughput as the number of nodes increases. This is due to the increasing probability of collision as the network size increases. Therefore, there have recently been many attempts aiming at establishing secure, dynamic, scheduled and collision-free protocols. Yet, as far as we know, non of the solutions proposed could achieve all these goals simultaneously. Most of the proposed solutions offer a certain service on the cost of loosing another. In the next section, we present a practical medium access scheme that achieves all these goals!

5.3 Advanced and Secure Medium Access Schemes

Contention-based protocols appeared firstly through ALOHA [112] and Slotted-ALOHA [113]. In pure ALOHA, a node accesses the channel whenever it has a packet to transmit regardless of the channel state. Yet, this mechanism leads to a high collision rate. In Slotted-ALOHA, the time is divided into discrete time slots and a node can only send at the beginning of a time slot. Although this decreases the collision rate, the latter remains high, especially in dense scenarios. To tackle this problem, carrier sense multiple access (CSMA) mechanisms have been developed. In CSMA, a node senses the channel before any transmission to avoid any interference with an ongoing transmission. The IEEE 802.11 DCF channel access technique is mainly based on the CSMA/CA mechanism with the RTS/CTS handshake. The collision avoidance mechanism through a random backoff, and the RTS/CTS handshake lead to a considerably higher bandwidth efficiency. Moreover, it incorporates the Binary Exponential Backoff (BEB) mechanism to evade consecutive collisions especially in congested networks with a high number of users. In BEB, the contention window is doubled whenever a collision occurs until reaching a maximum value and is reset to an initial value upon a successful transmission.

Many recent studies [114, 115, 116] have investigated the efficiency of the DCF channel access technique in congested wireless networks. In [114], the performance of DCF has been investigated analytically and through simulations. It has been shown that this technique performs well in small, lightly loaded networks but it exhibits a high collision rate in highly loaded and congested networks leading to a low efficiency.

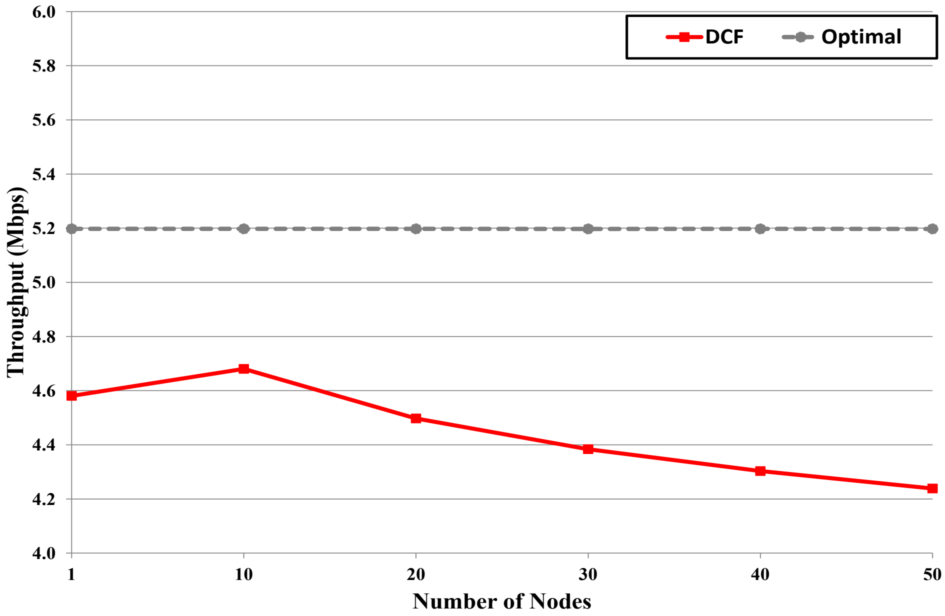


Figure 5.10: Throughput comparison between DCF and an optimal-scheduled channel access.

As a matter of fact, contention based channel access techniques do not achieve an optimal bandwidth efficiency compared to scheduled channel access even in low congested scenarios. This is mainly due to the contention period during which no data transmission occurs, in addition to the bandwidth loss due to collisions. To quantify the sub-optimality of contention-based techniques, we plot in Fig. 5.10 the total network throughput as a function of the number of nodes for the DCF technique and compare it to a theoretical throughput upper bound. The upper bound corresponds to the case of perfect scheduling between the nodes and hence a collision-free transmission[5,6].

[5] We assume that all the nodes are transmitting UDP traffic at high data rates.

[6] We do not discuss here the overhead due to the control packets, i.e. the theoretical throughput

We observe that there is a considerable throughput loss in using the DCF technique, mainly due to the contention period and the occurring collisions. This has also been analytically proved in [114, 115]. Therefore, there have been always an increasing interest in establishing scheduled collision-free medium access.

In this realm, polling schemes or centralized scheduling schemes have been proposed. Actually, the IEEE 802.11 standard includes the PCF mode as a polling scheme where the Access Point polls regularly the wireless stations. However, polling or centralized schemes are not practical in a dynamic scenario with a varying number of nodes and traffic rates. Therefore, distributed schemes have attracted more interest in wireless networks.

Indeed, the required features of an efficient and practical scheduling-based medium access scheme can be summarized by the following:

- Distributed: The scheduling or coordination between the nodes should be done in a distributed manner rather than a centralized coordinated manner.

- Dynamic: This means that the established schedule should adapt automatically to the network dynamics, such as the number of backlogged nodes, the different traffic rates, newly joining nodes, etc... Hence, the channel access scheme should provide a dynamic varying schedule according to the network dynamics instead of a fixed schedule.

- Efficient: An efficient channel access scheme should be collision-free or should minimize the number of collisions to avoid the loss of bandwidth due to collisions.

- Compatible (*Optional*): This property is mainly very important to establish a practical scheme compatible with the currently employed protocols. Schemes that require severe modifications to the packets formats or the communication protocols would be difficult to implement and receive wide acceptance.

- Misbehavior Resilient: Although the coordination between the nodes should be distributed, it should be somehow monitorable so that misbehavior detection can be easily performed at an AP or a centralized authority or watchdog nodes.

- Low Overhead: This property is a fundamental requirement towards achieving high efficiency in resource allocation. Any medium access technique incurring a large overhead leads to inefficiency in the usage of the limited network resources.

In this dissertation, we propose the Self-Organized Distributed Channel Access (SODCA) scheme that achieves all these goals and provides in high congestion states an

upper bound considered incorporates also the overhead of the MAC layer control packets.

efficiency very close to the theoretical upper bound corresponding to perfectly scheduled channel access. But before moving on to describe this scheme, we first describe briefly the recent and most important related work on this subject in the following section.

5.3.1 Related Work

There is a vast literature that investigates the DCF scheme and proposes more efficient channel access methods. In [117], Bharghavan et al. have proposed the MACAW scheme. In MACAW, a multiple-increase linear-decrease mechanism (MILD) is used instead of BEB to control the contention window size and hence reduce the number of collisions. On the other hand, Chatzimisios et al. have proposed a Double Increment Double Decrement (DIDD) mechanism [118]. The main difference between BEB and DIDD is that according to DIDD, the contention window is halved in case of a successful transmission. Whereas in BEB, it is reset to CW_{min}. Through simulations, it has been shown that DIDD outperforms BEB in a highly congested environment. This technique was more generalized by Song et al. in [119]. The authors in this paper have proposed an Exponential Increase Exponential Decrease (EIED) algorithm. In their algorithm, the contention window is multiplied by a parameter r_i upon collision and divided by a factor r_D upon a successful transmission. Simulation results have shown that EIED outperforms both BEB and MILD in terms of throughput and delay. Finally, Ye et al. have proposed a Multichain Backoff Mechanism (MCB) in [120]. In MCB, different backoff chains with different contention windows and parameters are defined. Hence, nodes adapt to the different congestion levels by switching between the multiple backoff chains. Simulation results have shown that this mechanism, though a little more complex, provides a higher throughput than MILD and EIED.

In [121], a history based adaptive backoff mechanism is proposed. In this scheme, the window size is adapted to the congestion history. Simulation results have shown that this approach outperforms BEB especially in a highly congested environment. Similarly, Zhu et al. derive, in [116], the optimal contention window size to be reset to, so that the oscillation in the contention window size is avoided and the channel utilization is maximized.

Ksentini et al. [122] have proposed a Deterministic Contention Window Algorithm (DCWA). It is based on introducing a lower bound on the contention window to separate between the different backoff ranges associated to the different contention stages. Moreover, the authors have proposed to adjust the backoff range according to the network load and past history to better reflect the contention state.

Cali et al. have investigated the p-persistent backoff algorithm in [123]. In this algorithm, the contention window size is tuned at runtime to obtain the maximum throughput. The authors have further discussed how the average contention window size that maximizes the performance can be estimated and hence dynamically tuned.

However, the optimal contention window cannot be easily and precisely estimated during run-time in some scenarios. This algorithm was analyzed and investigated also in [124].

Similarly, Bononi et al. [125] have proposed a distributed mechanism for contention window control in IEEE 802.11 networks where the contention window size is adapted to the current contention level. The mechanism, named Asymptotically Optimal Backoff (AOB), targets estimating the optimal contention window size which achieves the highest channel utilization. In AOB, the contention level is estimated using the slot utilization and the average size of the transmitted frames. Moreover, an additional level of control is added to the backoff mechanism so that a transmission is postponed in a probabilistic way in case the channel utilization exceeds the optimal value. The authors have performed simulations and they have showed that introducing AOB to IEEE 802.11 leads to a higher throughput. This work was further extended in [126] to enforce fairness in a heterogeneous network.

Determining a proper contention window size was also investigated by Liang et al. in [127]. In their paper, a Pause Count Backoff (PCB) algorithm was proposed to determine the proper backoff window size according to the network conditions. It is based on counting the number of backoff pauses to have an estimate of the number of active stations. Simulation results have demonstrated the effectiveness of this algorithm in comparison to DCF, EIED, and AEDCF [128].

Kwon et al. have proposed a Fast Collision Resolution (FCR) algorithm in [129]. In the FCR algorithm, both colliding and deferring stations update their contention window to avoid future collisions. As in IEEE 802.11 DCF, a station with a successful packet transmission resets its contention window to an initial value. However, the authors define a smaller minimum contention window than that in DCF. Moreover, the authors propose a fast exponential decrease of the backoff timer when a number of consecutive idle slots are detected. It has been shown that these changes reduce the average number of idle slots in a contention period, which leads to a throughput improvement. Finally, the authors incorporate the Self-Clocked Fair Queuing SCFQ algorithm [130] to establish a fairly scheduled FCR algorithm. Yet, the SCFQ algorithm targets achieving weighted fairness. This corresponds to distributing resources according to the weights of the flows as also investigated in [131, 132, 133, 134, 135, 136, 137].

Abichar et al. [138] have presented a distributed channel access scheme named CONTI. The scheme is based on the binary countdown mechanism and an elimination procedure. During each time slot, stations choose with a certain probability either to jam the medium or to refrain. Consequently, stations refraining and sensing a jammed medium quit the contention. The authors have showed that this elimination procedure is able to resolve contention in a limited number of time slots. They have compared this scheme with DCF and showed that it achieves a higher throughput and a lower collision rate. However, it has been found in [139] that this scheme may lead to a "contention deadlock problem". Nodes not hearing any jamming for a duration of DIFS would think that a new contention period has commenced. This leads ultimately to a new contention resolution period between all nodes. Finally, it is worthwhile to mention that the disadvantage of jamming schemes is that they lead to a high power consumption.

Based also on the elimination procedure, Zhou et al. [140] have designed a MAC protocol that can take the advantages of contention based and TDMA based protocols. It is based on the previously proposed k-EC (k-round Elimination Contention) [139]. In K-EC, the Contention Resolution Period (CRP) is divided into k contention rounds. During each round, some nodes are eliminated reaching finally one or more winners. An extension is proposed to resolve the case of more than one winner which leads ultimately to collision. The second phase guarantees that each backlogged node would have a unique contention vector. The authors argue that in the steady state each node will have a unique CV and hence scheduled collision-free transmission can occur. However, it is clear from their results that the elimination period is relatively large. In case of a dynamic network with nodes always leaving or joining, this procedure has to be repeated continuously which will eventually result in a large overhead. In fact, all presented results correspond to the steady state where perfect scheduled transmission is occurring without the need for the contention resolution. Yet, the case of a dynamic network has not been considered.

Apart from that, some other works have investigated Quality of Service (QoS) issues. In fact, QoS has been introduced through the EDCA scheme in IEEE 802.11e [141]. In EDCA, different traffic flows with different QoS requirements have been divided into access classes of different backoff parameters. Hence, all proposed approaches remain valid in case of contention between traffic flows corresponding to the same class. Therefore, for simplicity reasons, we do not consider QoS in this dissertation and leave this issue for future work.

In conclusion, most of the proposed solutions do not satisfy completely the main requirements for a practical and highly efficient medium access scheme. Some propose more efficient contention resolution but still offer a suboptimal efficiency. Whereas, most proposed scheduling solutions are only suitable for static scenarios and do not perform well in dynamic environments. Moreover, some of the proposed solutions require severe modifications and are not compatible with the current protocols. Finally, an important feature- misbehavior resilience- was not considered thoroughly in most of the proposed solutions. In the following, we describe our novel SODCA scheme that achieves these design goals.

5.3.2 The Self-Organized Distributed Channel Access Scheme

The Self-Organized Distributed Channel Access scheme targets establishing a schedule between the backlogged nodes in a distributed manner without the necessity of transmission of any information about the traffic rate, traffic type or queue length at any node. The basic idea behind this scheme is that each contending node winning a transmission opportunity defers until all other nodes get a transmission opportunity. This means that if the total number of backlogged nodes is known at any time, then each node, successfully getting channel access, should defer from the next transmission until all other stations have successfully got a transmission opportunity. The obtained schedule of transmission is then used in the following transmission rounds.

However, obtaining the total number of backlogged nodes is not trivial and incurs an additional overhead, especially in a dynamic network. To cope with this problem, we consider a maximum number N_{max} of nodes in the network and implement a method to detect the end of a schedule round when the total number of backlogged nodes is less than N_{max}. We define a schedule round as the period during which all backlogged nodes obtain a transmission opportunity. This means that a schedule round ends when N_{max} nodes have obtained a transmission opportunity or when the channel remains free for a duration equal to a Grant Transmission Window (GTW). A GTW is a duration during which a transmission is granted to the corresponding node in the schedule. Furthermore, we use the same CSMA/CA contention mechanism based on a Contention Window (CW) as in DCF, although we target a scheduled transmission. This resolves the problem of newly joining nodes. Indeed, newly joining nodes contend with the nodes in the current schedule during a CW leading ultimately to a newly obtained schedule for the next round. Hence, a GTW should be, by definition, greater than CW. Thus, the absence of a transmission during a GTW designates that the corresponding scheduled node has given up its turn (i.e. it has no packet in its transmission queue (non-backlogged) or it has quit the network).

5.3.2.1 Contention Window (CW)

Although we target establishing a scheduled transmission, contention between scheduled nodes and newly joining nodes cannot be avoided. This contention is mainly important at the phase of bootstrapping the network. In this phase, many backlogged nodes contend to establish a schedule. Therefore, we employ the same concept of contention based on CSMA/CA as in DCF. However, we define a smaller contention window size since contention happens rarely in SODCA and between very few contending nodes. We propose a minimal contention window size $CW_{min} = 4$ compared to 32 in DCF and a maximal contention window size $CW_{max} = 512$. Moreover, we use the same Binary Exponential Backoff (BEB) mechanism as in DCF for the purpose of compatibility. Actually, BEB has been proven to be efficient in decreasing the number of collisions and achieving a high throughput in *weakly* congested network states.

5.3.2.2 Grant Transmission Window (GTW)

A Grant Transmission Window (GTW) guarantees the opportunity of transmission for a scheduled node. Therefore, GTW should be greater than the contention window of all other nodes and should take into consideration all occurring own or overheard collisions in the network. An own collision can be simply detected by a timeout while waiting for a CTS packet. On the other hand, a collision between the RTS packets of other contending nodes can be detected by either hearing a noise over the channel or by detecting an RTS packet not followed by a CTS packet.

As with CW, we implement also a BEB mechanism to change the values of GTW according to the occurring collisions. Hence, GTW is doubled upon any occurring collision (own or overheard), until reaching a maximum value GTW_{max}. Moreover, GTW is set to GTW_{min} at the end of a schedule round as we will see later in the scheduling algorithm. Finally, we propose to set $GTW_{min} = 4$ and $GTW_{max} = 512$.

5.3.2.3 The SODCA algorithm

The question that remains is how to establish distributively a dynamic self-organized medium access. To achieve this goal, we introduce two parameters: the Turn Indicator (TI) and the Overheard Transmissions Counter (OTC). The TI parameter indicates the turn of a node in a schedule round. A value of 0 indicates that it is the turn of the node to transmit a packet and a value x different from 0 indicates that the node has to wait for x other transmissions before being allowed to transmit. The OTC parameter counts the number of transmissions by other nodes since the last own transmission. It is initialized by $N_{max} - 1$[7] to indicate the end of a schedule round and the start of a new one (i.e. N_{max} transmissions have already occurred). We note that these parameters are computed in a distributed way and are not exchanged between the nodes.

Whenever a node successfully obtains a transmission opportunity (in this case $TI = 0$)[8], it resets its parameters according to the two equations:

$$TI = N_{max} - 1 \tag{5.5}$$

$$OTC = OTC \ mod(N_{max} - 1) \tag{5.6}$$

[7] We also use OTC as a flag to differentiate between a node that has already transmitted during the current schedule round ($OTC < N_{max} - 1$) and a node that did not ($OTC \geq N_{max} - 1$)

[8] For simplicity of explanation, we consider that there is no packet loss due to channel conditions and hence we do not differentiate between a transmission opportunity and a successful collision-free transmission. However, a transmission opportunity (which we can represent by a CTS packet) is more appropriate to consider than a successful transmission in a real environment.

And upon overhearing a transmission by another node, it decrements the TI value (if greater than 0) and increments the OTC value until TI reaches 0. In the case where there are N_{max} backlogged nodes, the schedule round ends after N_{max} nodes[9] have obtained a transmission opportunity.

However, it might occur that the number of backlogged nodes during a schedule round is less than N_{max}. In this case, the end of a schedule round is detected by an idle GTW period. In fact, an idle GTW period signifies the end of a schedule period or a leaving node that was previously scheduled at the current turn. To differentiate between these two events for a node that has already had a transmission opportunity during the current round (i.e. $OTC < N_{max} - 1$), we estimate the number of backlogged nodes N_b during a schedule round. N_b can be simply estimated by the number of backlogged nodes during the last round. Hence, the end of a schedule round can be identified by comparing the number of nodes having already obtained a transmission opportunity, with the expected number of backlogged nodes. As a result, we have the following 3 cases:

- Case 1 ($N_{max} - 1 < OTC$): A node with $TI \neq 0$ and $N_{max} - 1 < OTC$ is a node that is scheduled for a later transmission in the current schedule round. Hence, an idle GTW signifies that an expected-backlogged node scheduled at the current turn has deferred from accessing the channel during its GTW (i.e. it has an empty transmission queue or has quit the network). Consequently, this node updates its turn indicator and the expected number of backlogged nodes, i.e TI and N_b are decremented by 1.

- Case 2 ($N_b - 1 \leq OTC < N_{max} - 1$): The case of $OTC \geq N_b$, means that all estimated backlogged nodes have already obtained a transmission opportunity. Whereas the case of $OTC = N_b - 1$ means that the last expected node in the schedule round has quit the transmission. In both cases, the end of the current schedule round is expected and the start of a new round is triggered. Hence, N_b, TI and OTC are updated according to the following equations:

$$N_b = OTC \tag{5.7}$$

$$TI = TI - (N_{max} - 1 - OTC) \tag{5.8}$$

$$OTC = N_{max} - 1 \tag{5.9}$$

- Case 3 ($OTC < N_b - 1$): A node falling into this case is a node that has already won a transmission opportunity during the current schedule round and has sensed an idle GTW. This means that an expected-backlogged node scheduled for the

[9] or $N_{max} - 1$ other nodes.

current round defers from accessing the channel during its GTW (i.e. it has an empty transmission queue or has quit the network). Moreover, $OTC < N_b - 1$ signifies that more backlogged nodes are expected to transmit during the current round (these would fall then into case 1)). Hence, the schedule round might not be over. Consequently, only N_b is decremented by 1.

Finally, GTW is reset to GTW_{min} whenever an idle GTW period is detected since all backlogged nodes will fall into one of these 3 cases.

The flowchart of the SODCA algorithm is shown in Fig. 5.11. As we can observe, a node enters either a contention state or a deferring state depending on its turn indicator:

- If $TI = 0$: it enters into contention. This state is quit only upon wining a transmission opportunity. In this case, TI and OTC are updated according to Eq. 5.5 and Eq. 5.6, respectively. And whenever any other contending node wins access to the channel, OTC is incremented by 1.

- If $TI \neq 0$: the node enters into a deferring state. Consequently, TI is decremented and OTC is incremented upon every overheard transmission until TI reaches 0. On the other hand, an idle GTW leads to one of the 3 cases discussed above.

Moreover, CW and GTW are updated based on the BEB mechanism. CW is doubled upon each collision encountered. Whereas GTW is doubled upon each collision encountered or overheard. We do not show this in the flowchart just for the purpose of simplicity of presentation.

Now that we have discussed the SODCA algorithm and the scheduling establishment mechanism, we can elaborate the following proposition:

Proposition 1. *If the total number of backlogged nodes is less than N_{max}, then according to the SODCA algorithm a collision-free scheduled transmission will be established in the steady state in a static congested network.*

Proof. See Fig. 5.12 for an example of 5 nodes (the steady state is reached at time instant t6). □

5.3.2.4 Joining Node

A node joining the network initializes the (TI, OTC) parameters to the values $(0, N_{max} - 1)$ and N_b to 0. This means that the node can directly transmit the packet (or contend on transmission of the packet) and start a new schedule round since $OTC = N_{max} - 1$, i.e. for this node the previous schedule round is over and all nodes have already obtained a transmission opportunity. This node contends with the currently scheduled

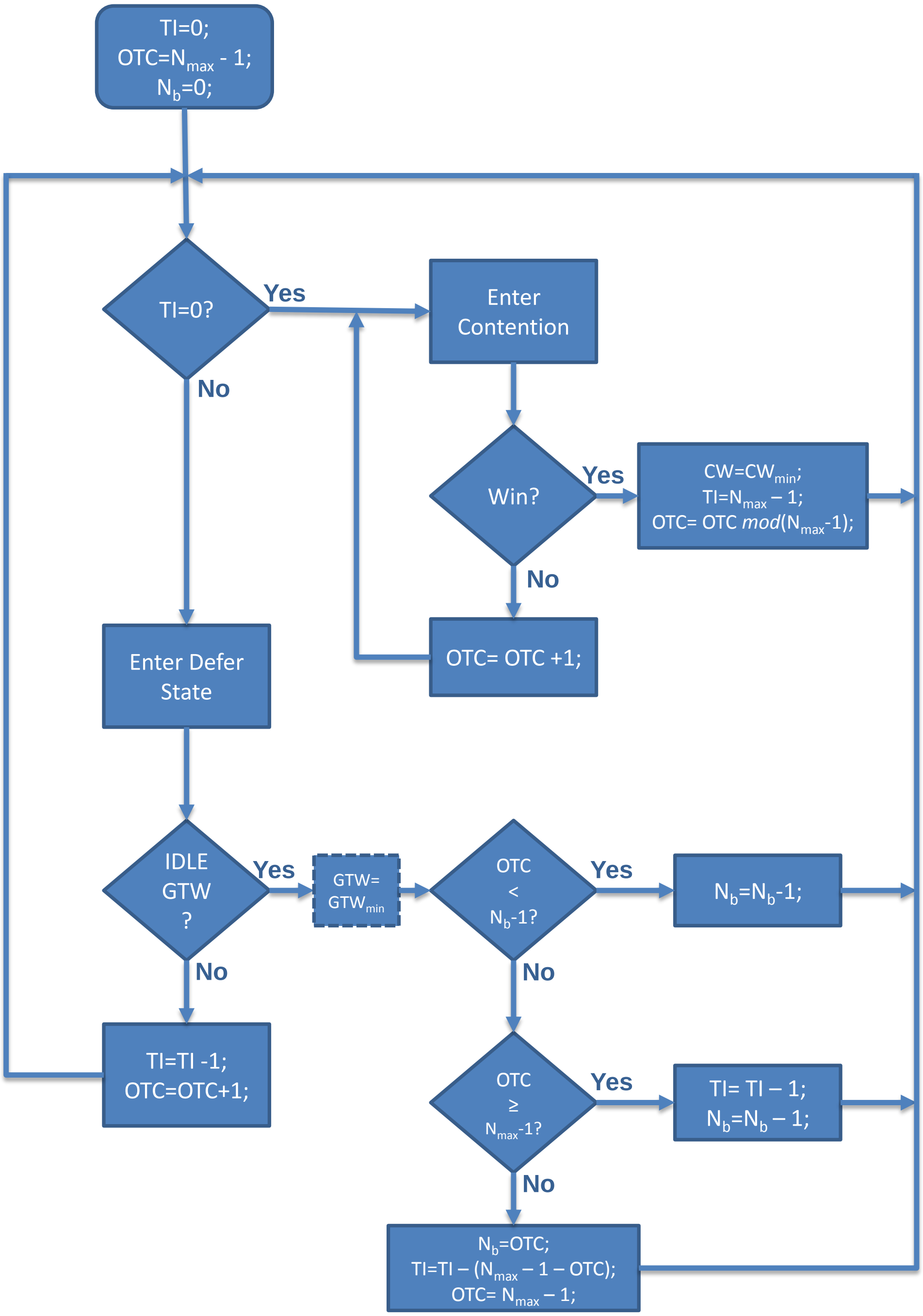
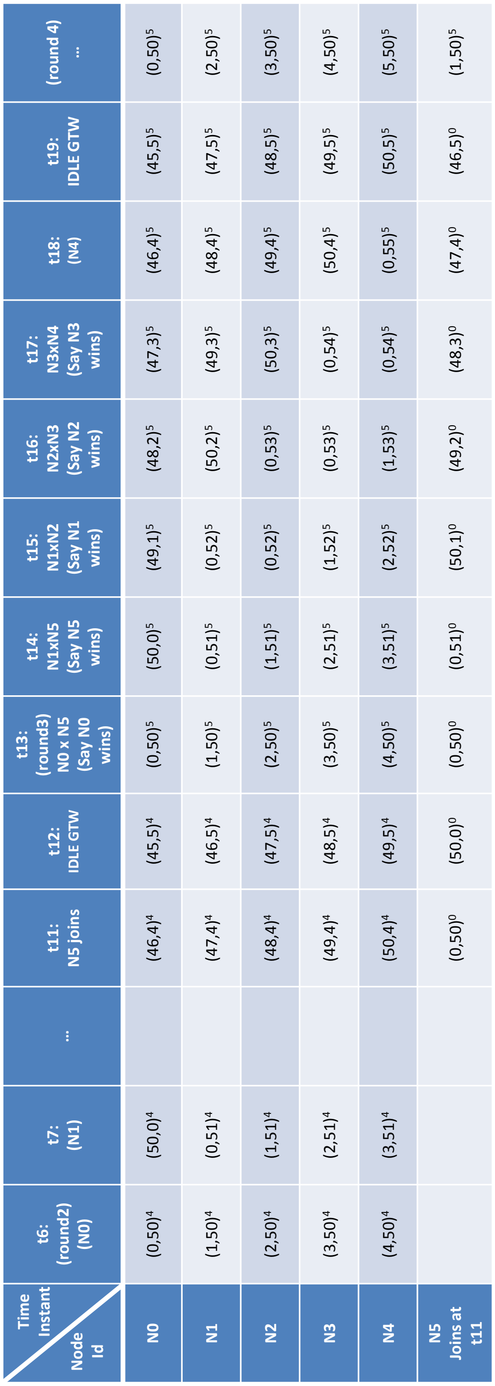


Figure 5.11: The flowchart of the SODCA algorithm (Collision events excluded).

Time Instant Node Id	t0: (N0)	t1: (N1)	t2: (N2)	t3: (N3)	t4: (N4)	t5: IDLE GTW	t6: (N0)	t7: (N1)	t8: (N2)	t9: (N3)	t10: (N4)	t11: IDLE GTW	...
N0	$(TI, OTC)^{Nb}$ $= (0,50)^0$	$(50,0)^0$	$(49,1)^0$	$(48,2)^0$	$(47,3)^0$	$(46,4)^0$	$(0,50)^4$	$(50,0)^4$	$(49,1)^4$	$(48,2)^4$	$(47,3)^4$	$(46,4)^4$	$(0,50)^4$
N1	$(0,50)^0$	$(0,51)^0$	$(50,1)^0$	$(49,2)^0$	$(48,3)^0$	$(47,4)^0$	$(1,50)^4$	$(0,51)^4$	$(50,1)^4$	$(49,2)^4$	$(48,3)^4$	$(47,4)^4$	$(1,50)^4$
N2	$(0,50)^0$	$(0,51)^0$	$(0,52)^0$	$(50,2)^0$	$(49,3)^0$	$(48,4)^0$	$(2,50)^4$	$(1,51)^4$	$(0,52)^4$	$(50,2)^4$	$(49,3)^4$	$(48,4)^4$	$(2,50)^4$
N3	$(0,50)^0$	$(0,51)^0$	$(0,52)^0$	$(0,53)^0$	$(50,3)^0$	$(49,4)^0$	$(3,50)^4$	$(2,51)^4$	$(1,52)^4$	$(0,53)^4$	$(50,3)^4$	$(49,4)^4$	$(3,50)^4$
N4	$(0,50)^0$	$(0,51)^0$	$(0,52)^0$	$(0,53)^0$	$(0,54)^0$	$(50,4)^0$	$(4,50)^4$	$(3,51)^4$	$(2,52)^4$	$(1,53)^4$	$(0,54)^4$	$(50,4)^4$	$(4,50)^4$

Figure 5.12: The evolution of the different parameters at network bootstrapping and during a schedule round (example of 5 backlogged nodes).



Time Instant / Node Id	t6: (round2) (N0)	t7: (N1)	...	t11: N5 joins	t12: IDLE GTW	t13: (round3) N0 x N5 (Say N0 wins)	t14: N1xN5 (Say N5 wins)	t15: N1xN2 (Say N1 wins)	t16: N2xN3 (Say N2 wins)	t17: N3xN4 (Say N3 wins)	t18: (N4)	t19: IDLE GTW	(round 4) ...
N0	$(0,50)^4$	$(50,0)^4$		$(46,4)^4$	$(45,5)^4$	$(0,50)^5$	$(50,0)^5$	$(49,1)^5$	$(48,2)^5$	$(47,3)^5$	$(46,4)^5$	$(45,5)^5$	$(0,50)^5$
N1	$(1,50)^4$	$(0,51)^4$		$(47,4)^4$	$(46,5)^4$	$(1,50)^5$	$(0,51)^5$	$(0,52)^5$	$(50,2)^5$	$(49,3)^5$	$(48,4)^5$	$(47,5)^5$	$(2,50)^5$
N2	$(2,50)^4$	$(1,51)^4$		$(48,4)^4$	$(47,5)^4$	$(2,50)^5$	$(1,51)^5$	$(0,52)^5$	$(0,53)^5$	$(50,3)^5$	$(49,4)^5$	$(48,5)^5$	$(3,50)^5$
N3	$(3,50)^4$	$(2,51)^4$		$(49,4)^4$	$(48,5)^4$	$(3,50)^5$	$(2,51)^5$	$(1,52)^5$	$(0,53)^5$	$(0,54)^5$	$(50,4)^5$	$(49,5)^5$	$(4,50)^5$
N4	$(4,50)^4$	$(3,51)^4$		$(50,4)^4$	$(49,5)^4$	$(4,50)^5$	$(3,51)^5$	$(2,52)^5$	$(1,53)^5$	$(0,54)^5$	$(0,55)^5$	$(50,5)^5$	$(5,50)^5$
N5 Joins at t11				$(0,50)^0$	$(50,0)^0$	$(0,50)^0$	$(0,51)^0$	$(50,1)^0$	$(49,2)^0$	$(48,3)^0$	$(47,4)^0$	$(46,5)^0$	$(1,50)^5$

Figure 5.13: The evolution of the different parameters when a backlogged node joins the network (example of 5 backlogged nodes).

node and the following ones. For this reason, the CSMA/CA contention mechanism is implemented. Finally, a new schedule is established for the next round.

In Fig. 5.13, we show the evolution of the TI, OTC and N_b parameters when a new backlogged node joins the network. We suppose that node $N5$ joins at t11 during which no node is scheduled (end of schedule). Hence, it can directly transmit its packet. In the next schedule round, it enters into contention with the first node. Ultimately, this contention will lead to a new schedule for the following schedule round. Similarly, a node joining at any instant during the schedule round will contend with the currently scheduled node and a new schedule would be established, in the worst case after two rounds. Therefore, we can elaborate the following proposition:

Proposition 2. *If a new backlogged node joins the network, a steady state of perfect collision-free scheduling will be established in a maximum of* 2 *rounds.*

5.3.2.5 Leaving Node

An already scheduled node might leave the network or enter into idle mode after its transmission queue is emptied. Other nodes detect this leaving node by an idle GTW. Thus, they react and update their parameters according to the scheduling algorithm described above.

In order to be able to join back the network, a node continues updating its parameters after sending its last packet in the transmission queue until reaching the initial value of $TI = 0$. Consequently, it resets all other parameters so that it can join the network later on as a newly joining node.

In Fig. 5.14, we show an example of 5 backlogged nodes where node $N2$ leaves the schedule round (it has an empty transmission queue or it has quit the network). We observe that the other nodes detect the absence of this node and reschedule their transmission accordingly. Consequently, a new schedule is established for the next schedule round. Based on this analysis, we can elaborate the following proposition:

Proposition 3. *If a node leaves the network, a steady state of perfect collision-free scheduling will be established in the next round.*

Now, based on Propositions 1, 2, and 3, we can elaborate the following corollary:

Corollary 1. *The SODCA scheduling algorithm is a dynamic scheduling algorithm.*

5.3.2.6 Misbehavior Detection in SODCA

Being a scheduling-based channel access scheme, SODCA facilitates misbehavior detection. In SODCA, a schedule is established in a self-organized, distributed and synchronized way, such that each node can have only one transmission opportunity per

Time Instant / Node Id	t6: (N0)	t7: (N1)	t8: IDLE GTW (N2 leaves)	t9: (N3)	t10: (N4)	t11: IDLE GTW	t12: (N0)	…
N0	$(TI, OTC)^{Nb}$ $=(0,50)^4$	$(50,0)^4$	$(49,1)^4$	$(49,1)^3$	$(48,2)^3$	$(47,3)^3$	$(0,50)^3$	…
N1	$(1,50)^4$	$(0,51)^4$	$(50, 1)^4$	$(50, 1)^3$	$(49, 2)^3$	$(48, 3)^3$	$(1,50)^3$	…
N2 Leaves at t8	$(2,50)^4$	$(1,51)^4$	~~(0,52)~~^{4}	X	X	X	X	…
N3	$(3,50)^4$	$(2,51)^4$	$(1,52)^4$	$(0,52)^3$	$(50,2)^3$	$(49,3)^3$	$(2,50)^3$	…
N4	$(4,50)^4$	$(3,51)^4$	$(2,52)^4$	$(1,52)^3$	$(0,53)^3$	$(50,3)^3$	$(3,50)^3$	…

Figure 5.14: The evolution of scheduling parameters when a node leaves a schedule round (example of 5 backlogged nodes).

schedule round. Hence, a misbehavior detection mechanism can be simply implemented by detecting any multiple transmissions by the same node during a schedule round. Consequently, a selfish node cannot get higher chances of channel access without being detected and hence, it is forced to adhere to the established schedule. Therefore, we can affirm that the SODCA scheme is resilient to misbehavior.

5.3.3 Simulation Results

To manifest the efficiency of the SODCA scheme compared to DCF, we have performed extensive simulations using the OMNeT++ network simulator based on the INET framework [110]. The system follows the IEEE 802.11b standard with 11Mbps maximum bit rate, a carrier frequency of 2.4GHz and a maximum transmission power of 20mW. The area size of the simulation topology is equal to 400 × 400 m^2, and all nodes are located at an equal distance from the access point in order to have a fair comparison of throughput distribution. Moreover, for the purpose of simplicity and to have a fair comparison, we consider a simple path-loss channel model. Finally, a maximum number of 51 nodes have been considered in the network, i.e. $N_{max} = 51$. However, SODCA is robust against any variations of this value, and any larger number would lead to approximately the same obtained results.

We have considered the case of constant bit rates at all nodes and a case of variable bit rates[10]. The former case corresponds to a static scenario, where a schedule is established and is continuously followed by all nodes. Whereas, the latter case corresponds to a dynamic scenario where the nodes are not always backlogged. We have performed simulations with various number of nodes and measured the total network throughput and the collision rate as a function of the number of nodes. We have performed 5 runs of each simulation, each for a duration of $500s$. Finally, the packet size is 1350 Bytes.

5.3.3.1 Constant Bit Rates (CBR)

To simulate a static scenario, we have considered high CBR traffic ($6Mbps$) at all nodes. Thus, all nodes are always backlogged and any established schedule would be always followed. In Fig. 5.15, we compare the total network throughput using SODCA or DCF and compare it to the upper bound. We observe that SODCA achieves a high total network throughput very close to the upper bound. Comparing to DCF, SODCA achieves up to 20% higher network throughput for a large number of nodes.

The collision rate in DCF and SODCA is compared in Fig. 5.16. We observe clearly that DCF leads to a high collision rate. On the other hand, the established schedule in channel access through SODCA leads to a negligible[11] collision rate.

[10] In both cases, a congested network state is considered.

[11] In this case, collisions only occur during bootstrapping the network and establishing the schedule.

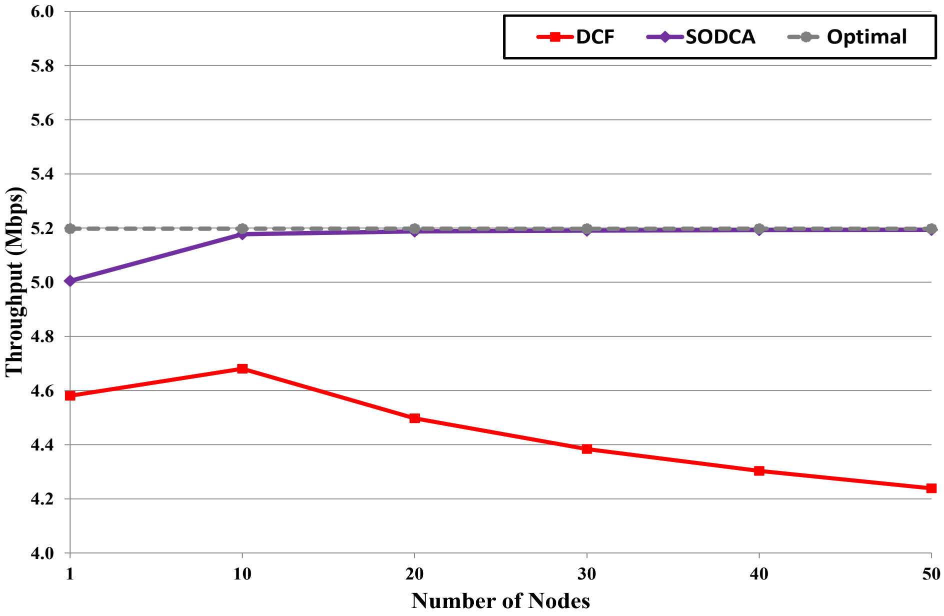
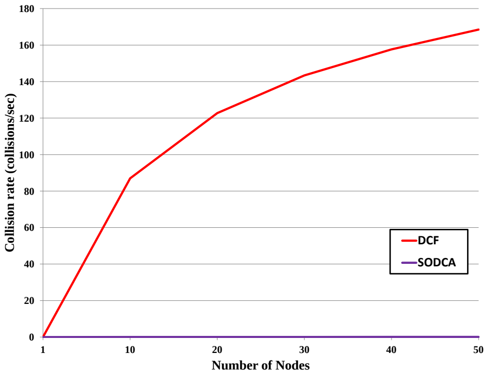


Figure 5.15: Total network throughput as a function of the number of nodes for DCF, SODCA and the optimal case, static scenario.



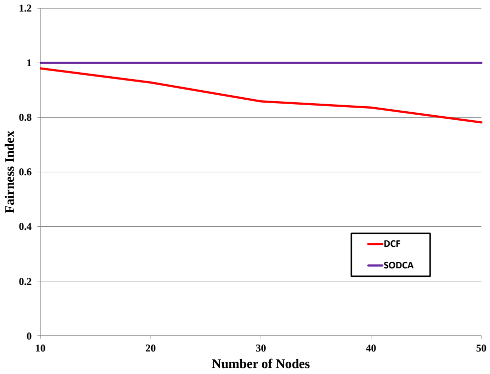


Figure 5.16: Collision rate of DCF and SODCA as a function of the number of nodes, static scenario.

Figure 5.17: Jain's fairness index comparison between DCF and SODCA, simulation time = 5s.

Finally, it is worth to note that DCF has a short-term fairness problem. To demonstrate this problem, we have performed simulations for a duration of $5s$ and calculated the Jain's fairness index. In Fig. 5.17, we plot the fairness index as a function of the number of nodes applying the DCF scheme and the SODCA scheme. We can observe clearly that DCF does not ensure a high fairness index whereas SODCA achieves a fairness index close to 100% even in a highly congested scenario.

5.3.3.2 Variable Bit Rates (VBR)

To simulate a dynamic scenario, we consider VBR traffic at the nodes. The total *average* bit rate considered is 5.4 $Mbps$, i.e. slightly higher than the maximal network throughput. In this scenario, the nodes will be joining and leaving continuously the established schedule according to their variable bit rates. Hence, the number of backlogged nodes will vary too, and an established schedule will be modified each round due to joining or leaving nodes. In a realistic scenario, wireless nodes get normally loaded by a burst of packets at a time, rather than one packet. Yet, we simulate this scenario to study the performance of SODCA in the worst cases.

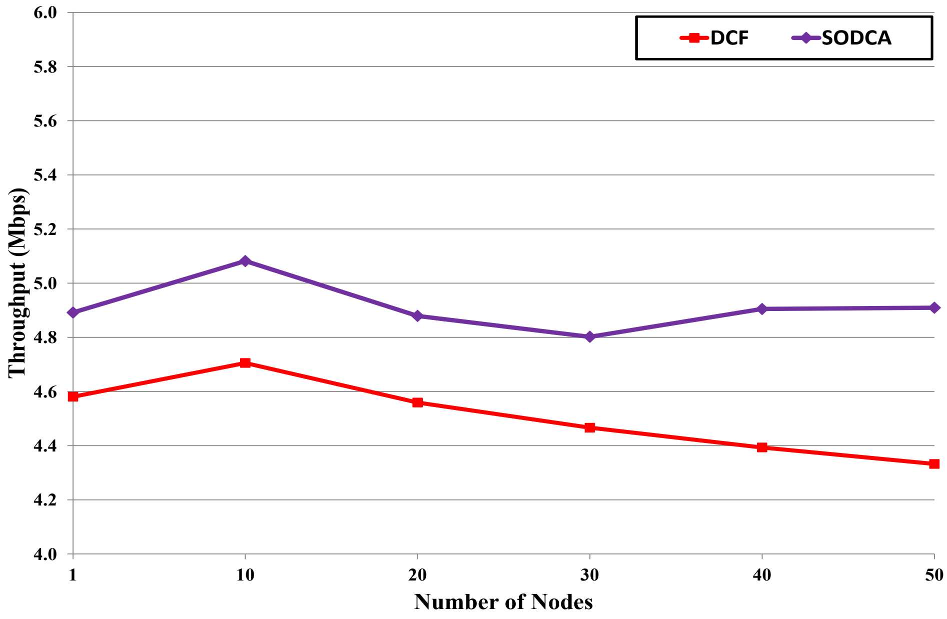


Figure 5.18: Total network throughput as a function of the number of nodes for the DCF and SODCA schemes, dynamic (VBR) scenario.

In Fig. 5.18, we trace the total network throughput as a function of the number of nodes for the DCF and SODCA schemes. We observe that SODCA still outperforms DCF. This is in fact due to the smaller contention window used and the efficient collision avoidance by a scheduled transmission. Indeed, we can observe clearly in Fig. 5.19, the significant difference in the collision rates between SODCA and DCF. SODCA results in at least 50% less collisions. We can conclude that our Self-Organized Distributed Channel Access scheme is very effective in reducing the collision rate and enhancing the bandwidth efficiency even in dynamic scenarios.

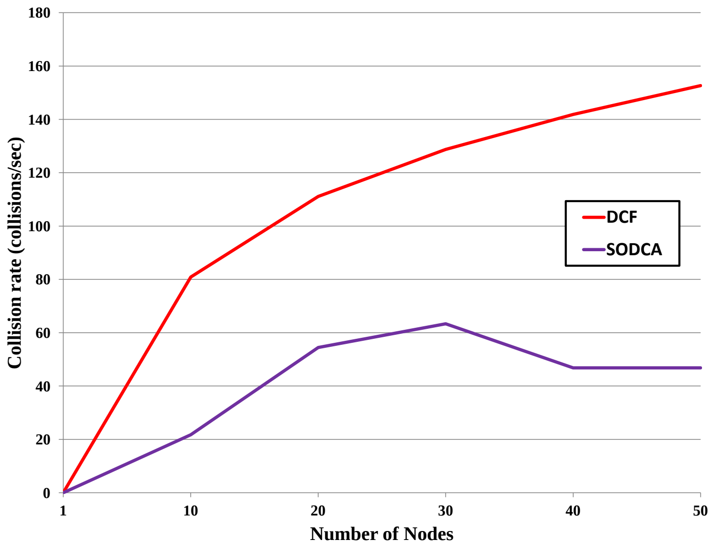


Figure 5.19: Collision rate as a function of the number of nodes for the DCF and SODCA schemes, dynamic (VBR) scenario.

5.3.4 Final Notes

5.3.4.1 Compatibility

The SODCA medium access scheme does not require any severe modifications to the DCF protocol. No modifications to the communication protocol, control frames, management frames, or data frames are required. Indeed, the main goal of this work was to organize the access to the channel so that the collision rate is minimized and hence the bandwidth efficiency is improved. Interestingly, SODCA manages to achieve this goal in a distributed manner without any exchange of information. This makes SODCA a practical solution and completely compatible with the current protocols.

5.3.4.2 Ad Hoc Mode

In the above simulations, we have considered for simplicity reasons the uplink traffic in a centralized network with an AP. However, the proposed medium access scheme suits best a 1-hop Ad Hoc network. In a 1-hop Ad Hoc network, all nodes are in communication range of each other. Hence, a self-organized medium access scheme would improve the total throughput of the network. An extension of the proposed scheme to multihop Ad Hoc networks is a target of our future work.

5.3.4.3 Power Consumption

Power conservation is one of the hidden properties of the SODCA scheme. Indeed, in SODCA, a backlogged node is not continuously in contention mode. It is only in contention mode in its scheduled turn during which it has a high chance of winning a transmission opportunity without any collision. This leads to a significantly lower power consumption. Moreover, the lower collision rate implies also a smarter use of both bandwidth and power resources.

5.4 Summary

In this chapter, we have investigated the efficiency and the security of the MAC layer in wireless networks. After an overview of the DCF medium access scheme, we discussed its vulnerability to different types of attacks. The backoff manipulation attack or the backoff misbehavior was mainly highlighted. It was shown that a node manipulating the random backoff procedure can deprive well-behaving nodes from network resources and get a higher share of the channel. After that, we presented our proposed Random Backoff Control (RBC) mechanism which allows MAC layer misbehavior detection. This mechanism is based on controlling the selection procedure of backoff values such that any node not obeying this procedure can be detected and penalized. Hence, nodes are forced to obey the RBC mechanism which ensures a fairer access to the common wireless channel. Our simulation results using OMNeT++ showed that the RBC mechanism is resilient against misbehavior and provides a fairer distribution of resources even in the presence of a selfish node applying an aggressive misbehaving strategy.

In the second part of this chapter, we have focused on elaborating efficient and secure medium access schemes. In fact, the efficiency of DCF has been largely investigated and compared to other proposed schemes in literature. Yet, as far as we know, no work has considered establishing an efficient and secure medium access scheme. To accomplish these two goals, we have explored distributed scheduling schemes. Intuitively, a scheduling scheme is expected to achieve higher efficiency due to lower collision rates, and a misbehavior resilience due to the established scheduled channel coordination.

Many scheduling-based access schemes have been proposed in literature, yet none of these have been found to be practical and well-suiting the current standards. Indeed, an effective medium access scheme should be distributed, dynamic, efficient, misbehavior resilient, compatible and should have a low overhead. Based on these required features, we have designed the Self-Organized Distributed Channel Access (SODCA) scheme. SODCA targets establishing a dynamic schedule in a distributed manner without requiring any modifications to the communication protocol. Through simulations using OMNeT++, SODCA has been proven to achieve a scheduled collision-free transmission in a static scenario. This results in a throughput gain up to 20% comparing to DCF. Moreover, SODCA has been investigated in a dynamic scenario where nodes have different variable bit rates. In this case, the number of backlogged nodes varies continuously and a new schedule needs to be established upon each joining or leaving node. SODCA has been proven to be capable of adapting dynamically the transmission schedule, hence achieving a higher performance than DCF, even in the worst case scenarios.

For future work, we would like first to extend the SODCA scheme and investigate it in multihop Ad hoc networks. In fact, we have considered only centralized and one hop Ad hoc networks in our study. Moreover, it would be very interesting to investigate Quality-of-Service (QoS) issues. Thus, a possible extension of SODCA is supporting QoS in a heterogeneous wireless network. Finally, we would like to note that the SODCA algorithm might have other applications that are worth investigation in queuing theory.

Chapter 6

Conclusions and Future Work

Contents

Security has been always considered on the upper layers of the wireless protocol suite, mainly at the network, transport and application layers. Subsequently, no much consideration has been given to the physical and MAC layers in securing wireless networks. Yet, the trend towards cross-layer design of security protocols has been continuously growing. In this dissertation, security issues and mechanisms at the lower layers in wireless networks have been investigated. We have first explored the potential of the physical layer in securing wireless communications, mainly through providing a secret key generation and agreement mechanism. On the other hand, we have tackled the problem of misbehavior in channel access and its impact on the distribution of channel resources, hence the importance of misbehavior detection and a secure medium access scheme.

6.1 Key Generation on the Physical Layer

In the first part of this dissertation, we have investigated key generation on the physical layer based on the wireless multipath channel. A brief review and analysis of some related work was first given. Most proposed key generation mechanisms have considered a 3 steps procedure based on a direct quantization of channel coefficients followed by reconciliation and finally privacy amplification. In contrary, we have developed smart quantization mechanisms achieving a high secret bit extraction rate at a low probability of error. Indeed, our proposed mechanisms are based on mitigating error in the quantization of the channel taps either through guard intervals (GI mechanism) or by shifting the phases of the channel taps synchronously (PS mechanism). The Guard Intervals (GI) quantization mechanism is mainly based on separating the quantization regions by guard intervals to mitigate errors. Whereas, the Phase Shifting (PS) quantization mechanism is mainly based on shifting the phases of the channel coefficients securely to approach the constellation points in order to improve the quantization performance. Moreover, optimal quantization parameters have been derived as a function of SNR to achieve a high efficiency of secret key extraction. Through simulation results, we have manifested the significant performance enhancements of these mechanisms over the direct quantization mechanism. Particularly, the PS quantization mechanism has been shown to achieve a high secret bit generation rate with more than 90 bits extracted per a single channel observation in a typical SISO outdoor channel model, at a low probability of key disagreement in the order of 10^{-3}. Furthermore, we have discussed using multiple antennas and a higher bandwidth to improve the secret bit generation rate.

After that, we have tackled some practical issues that affect the performance and reliability of key generation from the multipath wireless channel. Mainly, the effects of delay between the channel estimates and mobility have been investigated. Indeed, mobility leads to a varying channel. Hence, any delay in the channel estimation procedure at the two communicating nodes leads to different channel estimates obtained, and hence discrepancies in the derived secret bit streams. To tackle these two issues, we have developed the Enhanced 3-Way PS mechanism. The 3-way handshake procedure allows to model and correct the slight channel variation due to delay. Whereas, variation at higher mobility has been modeled as an added error that is then considered in the optimization process of the quantization parameters. This mechanism has been proven to be robust to delay and mobility while still achieving a high secret bit generation rate. Interestingly, we have also showed that mobility is in fact an advantage to our key generation mechanism as it allows a faster decorrelation of the channel and hence a faster re-application of the extraction mechanism to obtain a new secret bit stream. Indeed, the results obtained through simulations have showed that the overall secret key extraction rate increases as a function of mobility despite the negative effect of the channel variation on the average number of secret bits extracted from a single channel observation.

Finally, we have investigated reconciliation through error correcting codes, and key agreement which form the last stage of a key generation procedure. It has been shown that by applying an appropriate error correcting code, the key generation efficiency can be further enhanced while achieving an infinitesimally small probability of error, especially at low SNRs.

Our future work targets further improvements of the key generation rate through advanced joint encoding techniques. Moreover, it would be very interesting to test our proposed algorithms through real implementation and experimentation. In this case, some other issues need to be considered, as synchronization and frequency offset, to obtain a practical key generation mechanism.

6.2 Advanced and Secure Medium Access

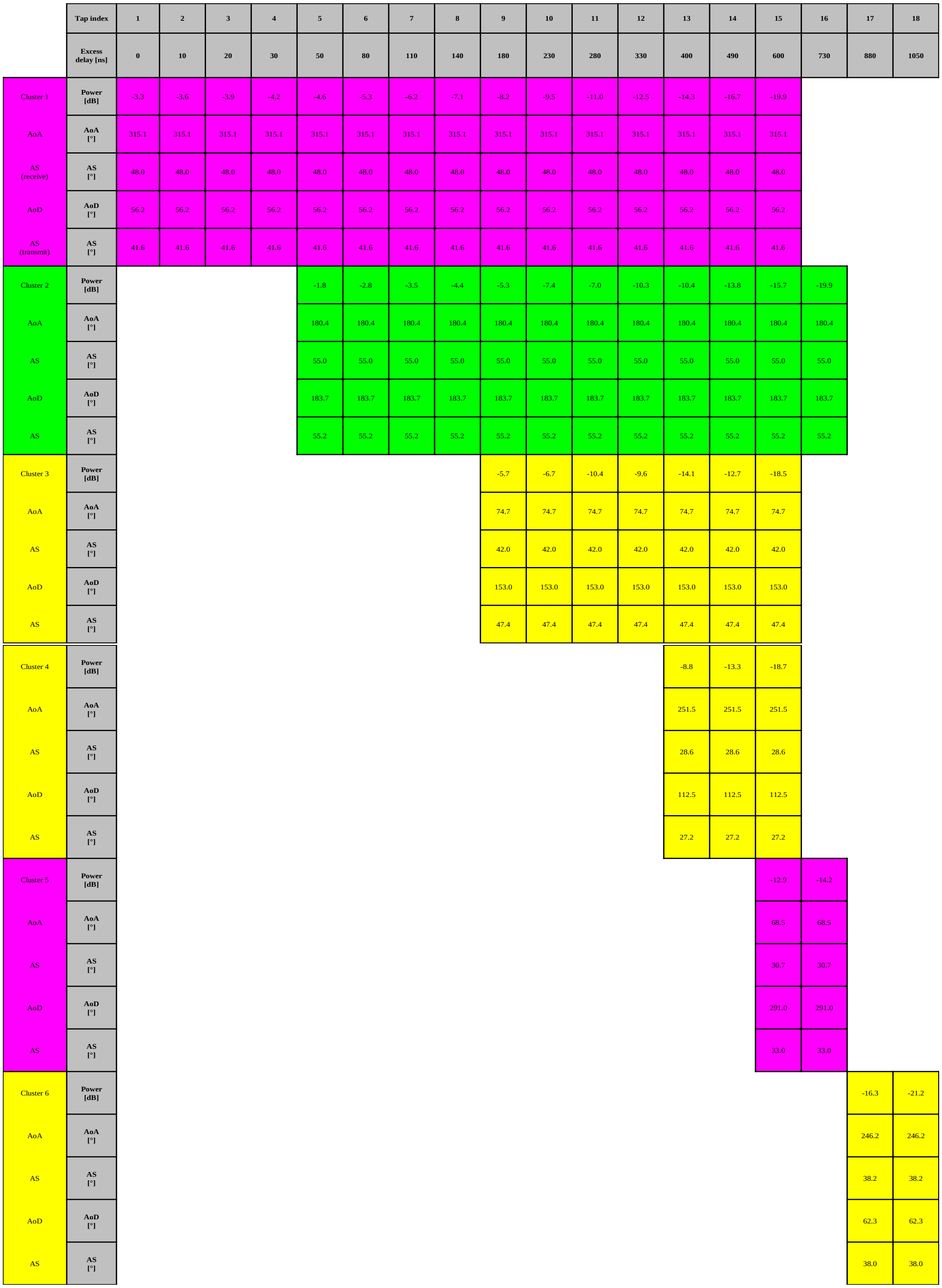
In the second part of this dissertation, we have investigated the efficiency and the security of the MAC layer in wireless networks. After an overview of the DCF medium access scheme, we discussed its vulnerability to different types of attacks. The backoff manipulation attack or the backoff misbehavior was mainly highlighted. It was shown that a node manipulating the random backoff procedure can deprive well-behaving nodes from network resources and get a higher share of the channel. After that, we presented our proposed Random Backoff Control (RBC) mechanism that allows misbehavior detection and mitigation. It is mainly based on controlling the selection procedure of backoff values by a dynamically varying lower bound such that any node not obeying this procedure is easily detected and penalized. Hence, nodes are forced to obey the RBC mechanism, which ensures a fairer access to the common wireless channel. Through simulation results, this mechanism has been proven to be effective in reducing significantly the effect of misbehavior, thus ensuring a fairer access to the channel even under aggressive attacks.

Afterwards, we have considered scheduling based medium access schemes. Intuitively, a scheduling based medium access scheme would result in a higher bandwidth efficiency due to the lower collision rate, and a resilience to misbehavior. After a revision of some of the most relevant work on this subject, we have presented our novel scheduling-based medium access scheme: the Self-Organized Distributed Channel Access (SODCA) scheme. Distinctively from all proposed schemes, SODCA is a distributed, efficient, compatible, misbehavior resilient and dynamic scheduling scheme. Moreover, it does not incur any additional overhead. Simulation results both in static and dynamic scenarios have affirmed the high efficiency of SODCA compared to contention based mechanisms. SODCA has been proven to achieve a scheduled collision-free transmission in a static scenario. This has resulted in a throughput gain up to 20% comparing to DCF. In a dynamic scenario, SODCA has been proven to be capable of adapting dynamically the transmission schedule, hence achieving a higher performance than contention-based medium access schemes. Finally, it is important to note that SODCA, by its design, mitigates selfish behavior on the MAC layer in wireless networks.

For future work, we would like first to extend the SODCA scheme and investigate it in multihop Ad hoc networks. In fact, we have considered only centralized and one hop Ad hoc networks in our study. Moreover, it would be very interesting to investigate Quality-of-Service (QoS) issues. Thus, a possible extension of SODCA is supporting QoS in a heterogeneous wireless network. Finally, we would like to note that the SODCA algorithm might have other applications that are worth investigation in queuing theory.

Appendix A

TGn Channel Model F



	Tap index	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	Excess delay [ns]	0	10	20	30	50	80	110	140	180	230	280	330	400	490	600	730	880	1050
Cluster 1	Power [dB]	-3.3	-3.6	-3.9	-4.2	-4.6	-5.3	-6.2	-7.1	-8.2	-9.5	-11.0	-12.5	-14.3	-16.7	-19.9			
AoA	AoA [°]	315.1	315.1	315.1	315.1	315.1	315.1	315.1	315.1	315.1	315.1	315.1	315.1	315.1	315.1	315.1			
AS (receive)	AS [°]	48.0	48.0	48.0	48.0	48.0	48.0	48.0	48.0	48.0	48.0	48.0	48.0	48.0	48.0	48.0			
AoD	AoD [°]	56.2	56.2	56.2	56.2	56.2	56.2	56.2	56.2	56.2	56.2	56.2	56.2	56.2	56.2	56.2			
AS (transmit)	AS [°]	41.6	41.6	41.6	41.6	41.6	41.6	41.6	41.6	41.6	41.6	41.6	41.6	41.6	41.6	41.6			
Cluster 2	Power [dB]					-1.8	-2.8	-3.5	-4.4	-5.3	-7.4	-7.0	-10.3	-10.4	-13.8	-15.7	-19.9		
AoA	AoA [°]					180.4	180.4	180.4	180.4	180.4	180.4	180.4	180.4	180.4	180.4	180.4	180.4		
AS	AS [°]					55.0	55.0	55.0	55.0	55.0	55.0	55.0	55.0	55.0	55.0	55.0	55.0		
AoD	AoD [°]					183.7	183.7	183.7	183.7	183.7	183.7	183.7	183.7	183.7	183.7	183.7	183.7		
AS	AS [°]					55.2	55.2	55.2	55.2	55.2	55.2	55.2	55.2	55.2	55.2	55.2	55.2		
Cluster 3	Power [dB]									-5.7	-6.7	-10.4	-9.6	-14.1	-12.7	-18.5			
AoA	AoA [°]									74.7	74.7	74.7	74.7	74.7	74.7	74.7			
AS	AS [°]									42.0	42.0	42.0	42.0	42.0	42.0	42.0			
AoD	AoD [°]									153.0	153.0	153.0	153.0	153.0	153.0	153.0			
AS	AS [°]									47.4	47.4	47.4	47.4	47.4	47.4	47.4			
Cluster 4	Power [dB]													-8.8	-13.3	-18.7			
AoA	AoA [°]													251.5	251.5	251.5			
AS	AS [°]													28.6	28.6	28.6			
AoD	AoD [°]													112.5	112.5	112.5			
AS	AS [°]													27.2	27.2	27.2			
Cluster 5	Power [dB]															-12.9	-14.2		
AoA	AoA [°]															68.5	68.5		
AS	AS [°]															30.7	30.7		
AoD	AoD [°]															291.0	291.0		
AS	AS [°]															33.0	33.0		
Cluster 6	Power [dB]																	-16.3	-21.2
AoA	AoA [°]																	246.2	246.2
AS	AS [°]																	38.2	38.2
AoD	AoD [°]																	62.3	62.3
AS	AS [°]																	38.0	38.0

Figure A.1: Parameters of the TGn channel model F [17].

Appendix B

Derivation of the Probability of Error

B.1 GI Mechanism

Lets consider h_1 as a channel estimate at Node 1 and h_2 as the corresponding channel estimate at Node 2. By considering only one tap, we can write:

$$h_2 = h_1 + z_2 - z_1 = h_1 + z', \tag{B.1}$$

where in this case h_1 is considered normalized, and z_1, z_2 are the independent added white Gaussian noises at both nodes which are supposed to be of equal power $\sigma^2 = 1/TNR$. Then, z' is the equivalent noise of power $2 \times \sigma^2$.

Let θ_1, θ_2 be the phases of h_1 and h_2, respectively. And let ϕ be the phase of z'. Then the probability of error can be expressed as the probability that θ_1 and θ_2 are in two different quantization regions.

Due to the uniform distribution of θ_1, this can be reduced to calculating the probability of error given that θ_1 is in the first region. In other words, for a guard phase of β and M quantization levels, it is the probability that $\theta_2 > \pi/M + \beta/2$ or $\theta_2 < -\pi/M - \beta/2$ given that $\theta_1 \in [(\text{-}\pi/M + \beta/2)\ (\pi/M - \beta/2)]$. This can be also approximated (for large TNR) as the probability of $\theta_2 > \pi/M + \beta/2$ given that $\theta_1 \in [0\ (\pi/M - \beta/2)]$.

From Fig. B.1, and for high TNR, one can write:

$$\tan(\Delta\theta) = \frac{x}{|h_1| + |z'|\cos(\phi - \theta_1)} \approx \frac{x}{|h_1|} = \frac{|z'|\sin(\phi - \theta_1)}{|h_1|}, \tag{B.2}$$

where $\Delta\theta$ is the phase difference due to noise, ϕ is the phase of the equivalent noise z', and θ_1 is the phase of h_1.

As z' follows $CN(0, 2\sigma^2)$ distribution, and as ϕ and θ_1 are uniformly distributed and independent, then $x = |z'|\sin(\phi - \theta_1)$ follows $N(0, \sigma^2)$ distribution. We also note that $|h_1| \approx 1$ as h_1 is normalized.

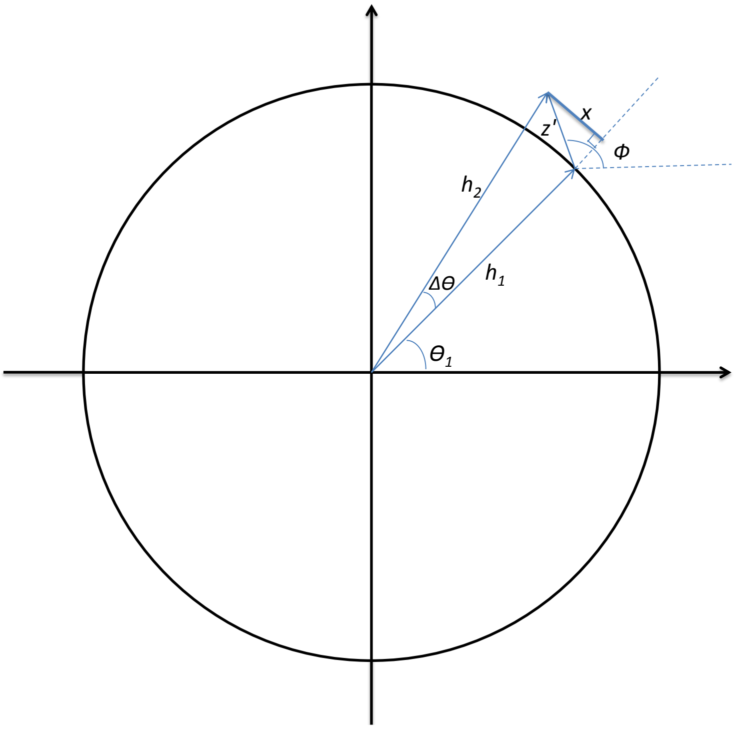


Figure B.1: Geometrical representation of the noisy channel estimates.

Consequently, we can write the probability of error as a function of θ_1 as

$$\begin{aligned} P_{\theta_1} &= P(\theta_2 > \frac{\pi}{M} + \frac{\beta}{2}) \\ &= P(\Delta\theta > \frac{\pi}{M} + \frac{\beta}{2} - \theta_1) \\ &= P(\tan(\Delta\theta) > \tan(\frac{\pi}{M} + \frac{\beta}{2} - \theta_1)), \end{aligned} \tag{B.3}$$

where β being always the guard phase, and M the number of quantization levels. By replacing $\tan(\Delta\theta)$ by x, we obtain:

$$P_{\theta_1} = P(x > \tan(\frac{\pi}{M} + \frac{\beta}{2} - \theta_1)), \tag{B.4}$$

which can be written in the form of the Error function:

$$P_{\theta_1} = \frac{1}{2} \cdot [1 - \mathrm{erf}(\frac{1}{\sqrt{2}\sigma} \tan(\frac{\pi}{M} - \theta_1 + \frac{\beta}{2}))], \tag{B.5}$$

Finally, the total probability of error can be found by integrating over the (reduced) range of θ_1:

$$P_{GI} = \frac{1}{\pi/M - \beta/2} \cdot \int_{\theta=0}^{\theta=\pi/M-\beta/2} P_\theta(\beta, M, \sigma) d\theta, \tag{B.6}$$

B.2 PS Mechanism

Applying the phase shifting method, we obtain the following relationship between the quantized phase estimate $\hat{\theta}$ and the phase-shifted estimate at node 2 θ_2':

$$\theta_2' = \Delta\theta + \hat{\theta}, \tag{B.7}$$

From this equation, we deduce that an error occurs using the PS mechanism if $|\Delta\theta|$ is large enough, i.e. if $|\Delta\theta| > \pi/M$. Based on this result, we can derive the probability of error in quantizing a channel tap as a function of TNR and M. However, in this case, we tend to use two different approximations in the high TNR region and the lower TNR region.

B.2.1 High TNR Region

For the case of a high TNR, we use a similar derivation as above and find that:

$$\begin{aligned} P_{PS} &= P(|\Delta\theta| > \frac{\pi}{M}) \\ &= P(\tan(|\Delta\theta|) > \tan(\frac{\pi}{M})), \end{aligned} \tag{B.8}$$

Again, by replacing $\tan(\Delta\theta)$ by x, we obtain:

$$P_{PS_{High}} = P(|x| > \tan(\frac{\pi}{M})), \tag{B.9}$$

which can be written in the form of the Error function:

$$P_{PS_{High}} = 1 - \text{erf}(\frac{1}{\sqrt{2}\sigma} \tan(\frac{\pi}{M})), \tag{B.10}$$

B.2.2 Low TNR Region

As for the low TNR region, the approximation made in (B.2) becomes inaccurate. Therefore, we follow a different procedure. First of all, we tend to assume in this case that the least quantization precision is used, i.e. $M = 2$. This means that an error occurs in the quantization process if $|\Delta\theta| > \pi/2$; or in other words if $\cos(\Delta\theta) < 0$. Based on this result, we can derive the probability of error in function of TNR and M.

Lets start first by expressing $\cos(\Delta\theta)$ in terms of $\cos(\Delta\theta_i)$ for $i = 1, 2$ where $\Delta\theta_i = \theta_i - \theta$.

$$\cos(\Delta\theta) = \cos(\Delta\theta_2 - \Delta\theta_1) = \cos(\Delta\theta_2) \cdot \cos(\Delta\theta_1) + \sin(\Delta\theta_2) \cdot \sin(\Delta\theta_1), \qquad \text{(B.11)}$$

where $\cos(\Delta\theta_i)$ and $\sin(\Delta\theta_i)$ in this case can be expressed as:

$$\cos(\Delta\theta_i) = \frac{|h| + |z_i| \cdot \cos(\phi_i - \theta_i)}{|h_i|}, \qquad \text{(B.12)}$$

$$\sin(\Delta\theta_i) = \frac{|z_i| \cdot \sin(\phi_i - \theta_i)}{|h_i|}, \qquad \text{(B.13)}$$

Taking into account that $|h| = 1$, we find out that $\cos(\Delta\theta) < 0$ implies:

$$(1 + x_1)(1 + x_2) + x_3 \cdot x_4 < 0, \qquad \text{(B.14)}$$

where $\gamma_i = \phi_i - \theta_i$, $x_1 = |z_1| \cos(\gamma_1)$, $x_2 = |z_2| \cos(\gamma_2)$, $x_3 = |z_1| \cdot \sin(\gamma_1)$, and $x_4 = |z_2| \cdot \sin(\gamma_2)$. In this case, x_1, x_2, x_3, and x_4 are i.i.d Gaussian random variables of variance $= \sigma^2/2$.

Based on these expressions, and after some mathematical derivations, we obtain an expression of the probability of error as:

$$P_{PS_{Low}} = P(x_1 < \frac{-x_3 \cdot x_4}{1 + x_2} - 1), \qquad \text{(B.15)}$$

Finally, using the Error function we can write:

$$P_{PS_{Low}} = \frac{1}{2}[1 + \cdot \oint \oint \oint \text{erf}(\frac{1}{\sigma} \cdot (-1 - \frac{y \cdot z}{1 + t})) \cdot P_y \cdot P_z \cdot P_t dydzdt], \qquad \text{(B.16)}$$

Appendix C
Security Analysis of QianWang2011

In the following, we analyze the security of the proposed key generation mechanism in [77] and prove that it is not secure against an adversary in the communication range of the two communicating nodes. Lets suppose that we have two rounds of key generation during the coherence time with equal phase shifts, where each node chooses a random initial phase during each round.
Let:
-θ_{12} be the channel phase shift between node S1 and node S2 ($\theta_{12} = \theta_{21}$).
-θ_{13} be the channel phase shift between node S1 and the eavesdropper.
-θ_{23} be the channel phase shift between node S2 and the eavesdropper.
-ϕ_1^i be the initial phase shift chosen by node S1 during round i.
-ϕ_2^i be the initial phase shift chosen by node S2 during round i.
We suppose that the eavesdropper is sufficiently separated from the communicating nodes, such that the channel phase shifts θ_{12}, θ_{13}, and θ_{23} are independent.

As a result, after two rounds and in absence of noise, each node will have:
• Nodes S1 and S2:
-Phase to be quantized in round 1: Φ^1=ϕ_1^1 + ϕ_2^1 + θ_{12} mod 2π
-Phase to be quantized in round 2: Φ^2=ϕ_1^2 + ϕ_2^2 + θ_{12} mod 2π

• Eavesdropper:
-Phases observed in round 1: α^1=ϕ_1^1 + θ_{13} mod 2π, and β^1=ϕ_2^1 + θ_{23} mod 2π
-Phases observed in round 2: α^2=ϕ_1^2 + θ_{13} mod 2π, and β^2=ϕ_2^2 + θ_{23} mod 2π

We notice here that: Φ^2=Φ^1 + α^2 - α^1 + β^2 - β^1 mod 2π
Since α^i's and β^i's are known, the phase obtained in the second round is directly correlated to the one in the first round for the Eavesdropper.

We conclude that the secret bits generated in multiple rounds are correlated for an eavesdropper, even sufficiently separated in space. As a result, only the bits generated in the first round can be considered secure, while others are directly correlated.

Bibliography

[1] Rolf Oppliger. *Contemporary Cryptography*. Artech House, Inc., Norwood, MA, USA, 2nd edition, 2011. (Cited on pages 2, 16 and 34.)

[2] Haowen Chan, Adrian Perrig, and Dawn Song. Random key predistribution schemes for sensor networks. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, SP '03, Washington, DC, USA, 2003. (Cited on pages 2 and 34.)

[3] Charles Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3–28, 1992. (Cited on pages 2 and 34.)

[4] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM international conference on Mobile computing and networking, MobiCom '08*, pages 128–139, New York, NY, USA, 2008. (Cited on pages 2, 34 and 38.)

[5] Chunxuan Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N.B. Mandayam. Information-theoretically secret key generation for fading wireless channels. *IEEE Transactions on Information Forensics and Security*, 5(2):240 –254, june 2010. (Cited on pages 2, 34 and 38.)

[6] Suman Jana, Sriram Nandha Premnath, Mike Clark, Sneha K. Kasera, Neal Patwari, and Srikanth V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of the 15th annual international conference on Mobile computing and networking, MobiCom '09*, pages 321–332, New York, NY, USA, 2009. (Cited on pages 2, 34, 38 and 39.)

[7] S. Premnath, S. Jana, J. Croft, P. Lakshmane Gowda, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy. Secret key extraction from wireless signal strength in real environments. *IEEE Transactions on Mobile Computing*, PP(99):1, 2012. (Cited on pages 2, 34, 38 and 39.)

[8] R. Wilson, D. Tse, and R. A. Scholtz. Channel identification: Secret sharing using reciprocity in ultrawideband channels. *IEEE Transactions on Information Forensics and Security*, 2(3):364 –375, sept. 2007. (Cited on pages 2, 34 and 42.)

[9] Jon Wallace. Secure physical layer key generation schemes: performance and information theoretic limits. In *Proceedings of the 2009 IEEE international conference on Communications*, ICC'09, pages 943–947, Piscataway, NJ, USA, 2009. (Cited on pages 2, 34, 43 and 48.)

[10] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, pages 1 –1076, 12 2007. (Cited on pages 3 and 71.)

[11] Lei Guang, C. Assi, and A. Benslimane. Enhancing IEEE 802.11 random backoff in selfish environments. *IEEE Transactions on Vehicular Technology*, 57(3):1806 –1822, may 2008. (Cited on pages 3, 72, 75, 79 and 81.)

[12] A. Rachedi and A. Benslimane. Smart attacks based on control packets vulnerabilities with IEEE 802.11 mac. In *International Wireless Communications and Mobile Computing Conference, IWCMC'08*, pages 588 –593, Aug. 2008. (Cited on pages 3, 72, 75 and 79.)

[13] Zhuo Lu, Wenye Wang, and Cliff Wang. On order gain of backoff misbehaving nodes in CSMA/CA-based wireless networks. In *Proceedings of the 29th conference on Information communications*, INFOCOM'10, pages 1819–1827, Piscataway, NJ, USA, 2010. (Cited on pages 3, 72 and 75.)

[14] William Stallings. *Network Security Essentials: Applications and Standards*. Prentice Hall Professional Technical Reference, 2nd edition, 2002. (Cited on pages 11, 13 and 16.)

[15] Whitfield Diffie and Martin E. Hellman. Multiuser cryptographic techniques. In *Proceedings of the 1976 national computer conference and exposition*, AFIPS '76, pages 109–112, New York, NY, USA, 1976. (Cited on page 16.)

[16] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall Press, Upper Saddle River, NJ, USA, 5th edition, 2010. (Cited on page 16.)

[17] V. Erceg et al. TGn channel models. *IEEE 802.11-03/940r4*, 2004. (Cited on pages 21, 30, 31, 57, 116 and 140.)

[18] Andrea Goldsmith. *Wireless Communications*. Cambridge University Press, New York, NY, USA, 2005. (Cited on pages 23, 24, 35, 43, 48 and 53.)

[19] David M. Pozar. *Microwave Engineering*. Wiley, 3rd edition. (Cited on page 26.)

[20] Constantine A. Balanis. *Antenna theory: analysis and design*. Wiley, 1982. (Cited on page 26.)

[21] C. A. Balanis. Antenna theory: a review. *Proceedings of the IEEE*, 80(1):7 –23, jan 1992. (Cited on page 26.)

[22] William C. Jakes and Donald C. Cox. *Microwave Mobile Communications*. Wiley-IEEE Press, 1994. (Cited on page 28.)

[23] Marius F. Pop and Norman C. Beaulieu. Limitations of sum-of-sinusoids fading channel simulators. *IEEE Trans. Commun*, pages 699–708, 2001. (Cited on page 28.)

[24] William C. Lee. *Mobile Communications Engineering*. McGraw-Hill Professional, 1982. (Cited on page 29.)

[25] A. M. Saleh and R. Valenzuela. A statistical model for indoor multipath propagation. *IEEE Journal on Selected Areas in Communications*, 5(2):128 –137, february 1987. (Cited on page 30.)

[26] Quentin H. Spencer, Michael D. Rice, and Michael A. Jensen. Modeling the statistical time and angle of arrival characteristics of an indoor multipath channel. *IEEE Journal on Selected Areas In Communications*, 18:347–360, 1996. (Cited on page 30.)

[27] R. Jean-Marc Cramer, Robert A. Scholtz, and Moe Z. Win. Evaluation of an ultra-wide-band propagation channel. *IEEE Trans. Antennas Propagation*, 50(5):561–570, 2002. (Cited on page 30.)

[28] Ada Poon and Minnie Ho. Indoor multiple-antenna channel characterization from 2 to 8 GHz. In *Proc. IEEE ICC*, 2003. (Cited on page 30.)

[29] A. Hassan. Cryptographic Key Agreement for Mobile Radio. *Digital Signal Processing*, 6(4):207–212, October 1996. (Cited on page 35.)

[30] Zang Li, Wenyuan Xu, Rob Miller, and Wade Trappe. Securing wireless systems via lower layer enforcements. In *Proceedings of the 5th ACM workshop on Wireless security, WiSe '06*, pages 33–42, New York, NY, USA, 2006. (Cited on pages 35 and 46.)

[31] S. Gollakota and D. Katabi. Physical layer wireless security made fast and channel independent. In *Proceedings IEEE INFOCOM '11*, pages 1125 –1133, april 2011. (Cited on pages 35 and 45.)

[32] http://www.ettus.com/. Usrp products. (Cited on page 35.)

[33] Yanpei Liu, Stark C. Draper, and Akbar M. Sayeed. A secret key generation system based on multipath channel randomness: RSSI vs CSI. *CoRR*, 2011. (Cited on page 36.)

[34] Ueli M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39:733–742, 1993. (Cited on page 36.)

[35] Rudolf Ahlswede and Imre Csiszár. Common randomness in information theory and cryptography - i: Secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, 1993. (Cited on page 36.)

[36] Amitav Mukherjee, S. Ali. A. Fakoorian, Jing Huang, and A. Lee Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *CoRR*, 2010. (Cited on page 36.)

[37] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. pages 410–423. Springer-Verlag, 1994. (Cited on page 37.)

[38] Matthieu Bloch, João Barros, Miguel R. D. Rodrigues, and Steven W. Mclaughlin. Wireless information-theoretic security - part I: Theoretical aspects. *IEEE Trans. on Information Theory*, 2006. (Cited on page 37.)

[39] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla. LDPC-based gaussian key reconciliation. In *IEEE Information Theory Workshop, ITW '06*, pages 116 –120, march 2006. (Cited on page 37.)

[40] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla. LDPC-based secret key agreement over the gaussian wiretap channel. In *IEEE International Symposium on Information Theory*, pages 1179 –1183, july 2006. (Cited on page 37.)

[41] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, 17(2):210–229, April 1988. (Cited on page 38.)

[42] C. H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915 –1923, nov 1995. (Cited on page 38.)

[43] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143 – 154, 1979. (Cited on page 38.)

[44] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.*, 22(3):265–279, 1981. (Cited on page 38.)

[45] U. Maurer and S. Wolf. Secret-key agreement over unauthenticated public channels–part III: Privacy amplification. *IEEE Transactions on Information Theory*, 49(4):839 – 851, April 2003. (Cited on page 38.)

[46] Yevgeniy Dodis, Jonathan Katz, and Leonid Reyzin. Robust fuzzy extractors and authenticated key agreement from close secrets. In *Advances in Cryptology–CRYPTO*, pages 232–250. Springer, 2006. (Cited on page 38.)

[47] Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, March 2008. (Cited on page 38.)

[48] Ran Raz, Omer Reingold, and Salil Vadhan. Extracting all the randomness and reducing the error in trevisan's extractors. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing, STOC '99*, pages 149–158, New York, NY, USA, 1999. (Cited on page 38.)

[49] Naom Nisan and Amnon Ta-Shma. Extracting randomness: a survey and new constructions. *J. Comput. Syst. Sci.*, 58(1):148–173, February 1999. (Cited on page 38.)

[50] Neal Patwari, Jessica Croft, Suman Jana, and Sneha K. Kasera. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Transactions on Mobile Computing*, 9(1):17–30, January 2010. (Cited on page 39.)

[51] Jessica Croft, Neal Patwari, and Sneha K. Kasera. Robust uncorrelated bit extraction methodologies for wireless sensors. In *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, IPSN '10*, pages 70–81, New York, NY, USA, 2010. (Cited on page 39.)

[52] Babak Azimi-Sadjadi, Aggelos Kiayias, Alejandra Mercado, and Bulent Yener. Robust key generation from signal envelopes in wireless networks. In *Proceedings of the 14th ACM conference on Computer and communications security, CCS '07*, pages 401–410, New York, NY, USA, 2007. (Cited on page 40.)

[53] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, March 2008. (Cited on page 40.)

[54] Matthias Wilhelm, Ivan Martinovic, and Jens B. Schmitt. On Key Agreement in Wireless Sensor Networks based on Radio Transmission Properties. In *Proceedings of the 5th Annual Workshop on Secure Network Protocols (NPSec '09)*, pages 37–42, October 2009. (Cited on page 40.)

[55] Matthias Wilhelm, Ivan Martinovic, and Jens B. Schmitt. Secret Keys from Entangled Sensor Motes: Implementation and Analysis. In *Proceedings of the Third ACM Conference on Wireless Network Security (WiSec '10)*, pages 139–144, March 2010. (Cited on page 40.)

[56] M.A. Forman and D. Young. A generalized scheme for the creation of shared secret keys through uncorrelated reciprocal channels in multiple domains. In *Proceedings of 18th International Conference on Computer Communications and Networks, ICCCN '09.*, pages 1 –8, aug. 2009. (Cited on page 40.)

[57] Sana Tmar-Ben Hamida, Jean-Benoît Pierrot, and Claude Castelluccia. An adaptive quantization algorithm for secret key generation using radio channel measurements. In *Proceedings of the 3rd international conference on New technologies, mobility and security, NTMS'09*, pages 59–63, Piscataway, NJ, USA, 2009. IEEE Press. (Cited on page 40.)

[58] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. *IEEE Transactions on Antennas and Propagation*, 53(11):3776 – 3784, nov. 2005. (Cited on page 40.)

[59] T. Aono, K. Higuchi, M. Taromaru, T. Ohira, and H. Sasaoka. Wireless secret key generation exploiting the reactance-domain scalar response of multipath fading channels : RSSI interleaving scheme. In *The European Conference on Wireless Technology*, pages 173 –176, oct. 2005. (Cited on pages 40 and 41.)

[60] A. Kitaura, H. Iwai, and H. Sasaoka. A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio. In *The 9th International Conference on Advanced Communication Technology*, volume 3, pages 1763 –1767, feb. 2007. (Cited on pages 40 and 41.)

[61] S. Yasukawa, H. Iwai, and H. Sasaoka. A secret key agreement scheme with multi-level quantization and parity check using fluctuation of radio channel property. In *IEEE International Symposium on Information Theory, ISIT '08*, pages 732 –736, july 2008. (Cited on pages 40 and 41.)

[62] FIPS PUB 140-2. Security Requirements for Cryptographic Modules, 2002. (Cited on page 41.)

[63] Kai Zeng, Daniel Wu, An Chan, and Prasant Mohapatra. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In *Proceedings of the 29th conference on Information communications, INFOCOM'10*, pages 1837–1845, Piscataway, NJ, USA, 2010. IEEE Press. (Cited on page 41.)

[64] Yunchuan Wei, Kai Zeng, and P. Mohapatra. Adaptive wireless channel probing for shared key generation. In *Proceedings IEEE INFOCOM 2011*, pages 2165 –2173, april 2011. (Cited on page 41.)

[65] Bin Zan, M. Gruteser, and Fei Hu. Improving robustness of key extraction from wireless channels with differential techniques. In *2012 International Conference on Computing, Networking and Communications (ICNC'12)*, pages 980 –984, feb. 2012. (Cited on page 42.)

[66] Hongbo Liu, Jie Yang, Yan Wang, and Yingying Chen. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In *2012 Proceedings IEEE INFOCOM*, pages 927 –935, march 2012. (Cited on page 42.)

[67] Chunxuan Ye, A. Reznik, and Y. Shah. Extracting secrecy from jointly gaussian random variables. In *IEEE International Symposium on Information Theory*, pages 2593 –2597, july 2006. (Cited on page 43.)

[68] Chunxuan Ye, A. Reznik, G. Sternberg, and Y. Shah. On the secrecy capabilities of ITU channels. In *IEEE 66th Vehicular Technology Conference, VTC-Fall 2007*, pages 2030 –2034, oct. 2007. (Cited on pages 43 and 48.)

[69] 3GPP. User equipment (UE) radio transmission and reception (FDD) (Release 6), 2005. (Cited on page 43.)

[70] A. Sayeed and A. Perrig. Secure wireless communications: Secret keys through multipath. In *IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP '08*, pages 3013 –3016, april 2008. (Cited on page 43.)

[71] Xiaojun Sun, Wei Xu, Ming Jiang, and Chunming Zhao. Improved generation efficiency for key extracting from wireless channels. In *IEEE International Conference on Communications (ICC '11)*, pages 1 –6, june 2011. (Cited on page 43.)

[72] Xiaojun Sun, Xiaofu Wu, Chunming Zhao, Ming Jiang, and Wei Xu. Slepian-wolf coding for reconciliation of physical layer secret keys. In *Proceedings IEEE Wireless Communications and Networking Conference (WCNC '10)*, pages 1 –6, april 2010. (Cited on page 43.)

[73] J.W. Wallace, Chan Chen, and M.A. Jensen. Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits. In *3rd European Conference on Antennas and Propagation, EuCAP 2009*, pages 1499 –1503, march 2009. (Cited on page 43.)

[74] J.W. Wallace and R.K. Sharma. Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis. *IEEE Transactions on Information Forensics and Security*, 5(3):381 –392, sept. 2010. (Cited on page 43.)

[75] Chan Chen and M.A. Jensen. Random number generation from multipath propagation: MIMO-based encryption key establishment. In *IEEE International Symposium on Antennas and Propagation Society, APSURSI '09*, pages 1 –4, june 2009. (Cited on page 44.)

[76] Chan Chen and M.A. Jensen. Secrecy extraction from increased randomness in a time-variant MIMO channel. In *IEEE Global Telecommunications Conference,GLOBECOM '09*, pages 1 –6, dec. 2009. (Cited on page 44.)

[77] Qian Wang, Hai Su, Kui Ren, and Kwangjo Kim. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In *Proceedings IEEE INFOCOM '11*, pages 1422 –1430, april 2011. (Cited on pages 44 and 121.)

[78] Qian Wang, Kaihe Xu, and Kui Ren. Cooperative secret key generation from phase estimation in narrowband fading channels. *CoRR*, 2011. (Cited on page 44.)

[79] Kui Ren, Hai Su, and Qian Wang. Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wireless Communications*, 18(4):6 –12, august 2011. (Cited on page 44.)

[80] Tzu-Han Chou, S.C. Draper, and A.M. Sayeed. Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness. In *Proceedings IEEE International Symposium on Information Theory (ISIT '10)*, pages 2518 –2522, june 2010. (Cited on page 44.)

[81] WenJie Wang, HongYan Jiang, XiangGen Xia, PengCheng Mu, and QinYe Yin. A wireless secret key generation method based on chinese remainder theorem in FDD systems. *SCIENCE CHINA Information Sciences*, 55:1605–1616, 2012. (Cited on page 44.)

[82] T. Kitano, A. Kitaura, H. Iwai, and H. Sasaoka. A private key agreement scheme based on fluctuations of BER in wireless communications. In *The 9th International Conference on Advanced Communication Technology*, volume 3, pages 1495 –1499, feb. 2007. (Cited on page 45.)

[83] G.R. Tsouri and D. Wulich. Reverse piloting protocol for securing time varying wireless channels. In *Wireless Telecommunications Symposium,WTS '08*, pages 125 –131, april 2008. (Cited on page 45.)

[84] Bin Zan and M. Gruteser. Random channel hopping schemes for key agreement in wireless networks. In *Proc. of the 20th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC '09*, pages 2886 –2890, sept. 2009. (Cited on page 45.)

[85] Kai Zeng, K. Govindan, and P. Mohapatra. Non-cryptographic authentication and identification in wireless networks. *IEEE Wireless Communications*, 17(5):56 –62, october 2010. (Cited on page 46.)

[86] S. Mathur, A. Reznik, Chunxuan Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam. Exploiting the physical layer for enhanced security. *IEEE Wireless Communications*, 17(5):63 –70, october 2010. (Cited on page 46.)

[87] Liang Xiao, L. Greenstein, N. Mandayam, and W. Trappe. Fingerprints in the ether: Using the physical layer for wireless authentication. In *IEEE International Conference on Communications, ICC '07*, pages 4646 –4651, june 2007. (Cited on page 46.)

[88] Youssef El Hajj Shehadeh and Dieter Hogrefe. An optimal guard-intervals based mechanism for key generation from multipath wireless channels. In *The 4th IEEE International Conference on New Technologies, Mobility and Security (NTMS 11)*, Paris, France, February 2011. (Cited on page 48.)

[89] Youssef El Hajj Shehadeh, Omar Alfandi, Kifah Tout, and Dieter Hogrefe. Intelligent mechanisms for key generation from multipath wireless channels. In *The 10th IEEE Wireless Telecommunications Symposium (WTS 2011)*, New York, USA, April 2011. (Cited on page 48.)

[90] Youssef El Hajj Shehadeh and Serdar Sezginer. Fast varying channel estimation in downlink LTE systems. In *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC '10*, pages 608–613, 2010. (Cited on pages 48, 49 and 62.)

[91] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. *IEEE Std 802.11n-2009 (Amendment to IEEE*

Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009), pages 1 –565, 2009. (Cited on page 57.)

[92] A. Rahman and P. Gburzynski. Hidden problems with the hidden node problem. In *23rd Biennial Symposium on Communications*, pages 270 –273, 2006. (Cited on pages 73, 77 and 78.)

[93] Abderrezak Rachedi and Abderrahim Benslimane. Impacts and solutions of control packets vulnerabilities with IEEE 802.11 MAC. *International Wireless Communications and Mobile Computing Conference, IWCMC'09*, 9(4), April 2009. (Cited on pages 75, 79 and 89.)

[94] Maxim Raya, Jean-Pierre Hubaux, and Imad Aad. DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services- MobiSys'04*, MobiSys '04, pages 84–97, New York, NY, USA, 2004. (Cited on pages 75, 76, 77 and 80.)

[95] Y. Zhou, D. Wu, and S.M. Nettles. Analyzing and preventing MAC-layer denial of service attacks for stock 802.11 systems. In *Proceedings of the IEEE Workshop on Broadband Wireless Services and Applications (BWSA'04)*, pages 270 –273, San Jose, Calif, USA, 2004. (Cited on pages 75 and 89.)

[96] P. Kyasanur and N.H. Vaidya. Detection and handling of MAC layer misbehavior in wireless networks. In *Proc. International Conference on Dependable Systems and Networks*, pages 173 – 182, june 2003. (Cited on pages 75 and 79.)

[97] Lei Guang and C. Assi. Mitigating smart selfish MAC layer misbehavior in Ad Hoc networks. In *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications- WIMOB'06*, WIMOB '06, Washington, DC, USA, 2006. (Cited on pages 75, 80, 81 and 82.)

[98] John Bellardo and Stefan Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *Proceedings of the USENIX Security Symposium*, page 15–28, Washington, D.C., August 2003. (Cited on pages 75 and 77.)

[99] Zhiguo Zhang, Jingqi Wu, Jing Deng, and Meikang Qiu. Jamming ACK attack to wireless networks and a mitigation approach. In *GLOBECOM*, pages 4966–4970, 2008. (Cited on page 77.)

[100] P. Kyasanur and N.H. Vaidya. Selfish MAC layer misbehavior in wireless networks. *IEEE Transactions on Mobile Computing*, 4(5):502–516, 2005. (Cited on page 79.)

[101] Alvaro A. Cárdenas, Svetlana Radosavac, and John S. Baras. Detection and prevention of MAC layer misbehavior in Ad hoc networks. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, SASN '04, pages 17–22, New York, NY, USA, 2004. (Cited on pages 79 and 80.)

[102] Vamshikrishna Reddy Giri and Neeraj Jaggi. MAC layer misbehavior effectiveness and collective aggressive reaction approach. In *Proceedings of the 33rd IEEE conference on Sarnoff*, Sarnoff'10, pages 200–204, Piscataway, NJ, USA, 2010. (Cited on pages 79 and 89.)

[103] N. Jaggi, V.R. Giri, and V. Namboodiri. Distributed reaction mechanisms to prevent selfish misbehavior in wireless Ad Hoc networks. In *IEEE Global Telecommunications Conference (GLOBECOM 2011)*, pages 1 –6, dec. 2011. (Cited on pages 79 and 89.)

[104] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux. On selfish behavior in CSMA/CA networks. In *Proceedings IEEE INFOCOM 2005*, volume 4, pages 2513 – 2524 vol. 4, march 2005. (Cited on pages 79 and 89.)

[105] A. Venkatarama, Cherita L. Corbett, and Raheem A. Beyah. A wired-side approach to MAC misbehavior detection. In *ICC*, pages 1–6, 2010. (Cited on page 79.)

[106] Maxim Raya, Imad Aad, Jean-Pierre Hubaux, and Alaeddine El Fawal. DOMINO: Detecting mac layer greedy behavior in IEEE 802.11 hotspots. *IEEE Transactions on Mobile Computing*, 5(12):1691–1705, 2006. (Cited on page 80.)

[107] A.A. Cardenas, S. Radosavac, and J.S. Baras. Performance comparison of detection schemes for mac layer misbehavior. In *IEEE International Conference on Computer Communications INFOCOM 2007*, pages 1496 –1504, may 2007. (Cited on page 80.)

[108] Alvaro A. Cárdenas, Svetlana Radosavac, and John S. Baras. Evaluation of detection algorithms for MAC layer misbehavior: theory and experiments. *IEEE/ACM Trans. Netw.*, 17(2):605–617, April 2009. (Cited on page 80.)

[109] Y. Rong, S.-K. Lee, and H.-A. Choi. Detecting stations cheating on backoff rules in 802.11 networks using sequential analysis. In *Proceedings IEEE International Conference on Computer Communications, INFOCOM 2006*, pages 1 –13, april 2006. (Cited on page 80.)

[110] http://inet.omnetpp.org/. (Cited on pages 84 and 105.)

[111] R. Jain. *The Art of Computer Systems Performance Analysis*. John Wiley and sons, New York, NY, USA, 1991. (Cited on page 88.)

[112] Norman Abramson. The ALOHA system: another alternative for computer communications. In *Proceedings of the fall joint computer conference*, AFIPS '70 (Fall), pages 281–285, New York, NY, USA, 1970. (Cited on page 90.)

[113] Lawrence G. Roberts. ALOHA packet system with and without slots and capture. *SIGCOMM Comput. Commun. Rev.*, 5(2):28–42, April 1975. (Cited on page 90.)

[114] G. Bianchi. Performance analysis of the IEEE 802.11 distributed coordination function. *IEEE J.Sel. A. Commun.*, 18(3):535–547, September 2000. (Cited on pages 91 and 92.)

[115] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda. Performance anomaly of 802.11b. In *IEEE INFOCOM 2003*, volume 2, pages 836 – 843, april 2003. (Cited on pages 91 and 92.)

[116] Yi-Hua Zhu, Xian-Zhong Tian, and Jun Zheng. Performance analysis of the binary exponential backoff algorithm for IEEE 802.11 based mobile Ad Hoc networks. In *IEEE International Conference on Communications (ICC) 2011*, pages 1 –6, june 2011. (Cited on pages 91 and 93.)

[117] Vaduvur Bharghavan, Alan Demers, Scott Shenker, and Lixia Zhang. MACAW: a media access protocol for wireless LANs. In *Proceedings of the conference on Communications architectures, protocols and applications*, SIGCOMM '94, pages 212–225, New York, NY, USA, 1994. (Cited on page 93.)

[118] P. Chatzimisios, V. Vitsas, and A. C. Boucouvalas. On improving performance for IEEE 802.11 wireless LANs under congested and error-prone environments. In *Proceedings of the 24th IASTED international conference on Internet and multimedia systems and applications*, IMSA'06, pages 177–182, Anaheim, CA, USA, 2006. (Cited on page 93.)

[119] Nah-Oak Song, Byung-Jae Kwak, Jabin Song, and M.E. Miller. Enhancement of IEEE 802.11 distributed coordination function with exponential increase exponential decrease backoff algorithm. In *IEEE VTC 2003-Spring*, volume 4, pages 2775 –2778 vol.4, april 2003. (Cited on page 93.)

[120] Shiang-Rung Ye and Yu-Chee Tseng. A multichain backoff mechanism for IEEE 802.11 WLANs. *IEEE Transactions on Vehicular Technology*, 55(5):1613 –1620, sept. 2006. (Cited on page 93.)

[121] Q. Nasir and M. Albalt. Improved backoff algorithm for IEEE 802.11 networks. In *International Conference on Networking, Sensing and Control, ICNSC '09*, pages 1 –6, march 2009. (Cited on page 93.)

[122] A. Ksentini, A. Nafaa, A. Gueroui, and M. Naimi. Determinist contention window algorithm for IEEE 802.11. In *IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2005*, volume 4, pages 2712 –2716 Vol. 4, sept. 2005. (Cited on page 93.)

[123] Frederico Calì, Marco Conti, and Enrico Gregori. Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit. *IEEE/ACM Trans. Netw.*, 8(6):785–799, December 2000. (Cited on page 93.)

[124] Der-Jiunn Deng, Chih-Heng Ke, Hsiao-Hwa Chen, and Yueh-Min Huang. Contention window optimization for IEEE 802.11 DCF access control. *Trans. Wireless. Comm.*, 7(12):5129–5135, December 2008. (Cited on page 94.)

[125] Luciano Bononi, Marco Conti, and Enrico Gregori. Runtime optimization of IEEE 802.11 wireless LANs performance. *IEEE Trans. Parallel Distrib. Syst.*, 15(1):66–80, January 2004. (Cited on page 94.)

[126] Raffaele Bruno, Marco Conti, and Enrico Gregori. Distributed contention control in heterogeneous 802.11b WLANs. In *Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services*, WONS '05, pages 190–199, Washington, DC, USA, 2005. (Cited on page 94.)

[127] Hao-Ming Liang, Sherali Zeadally, Naveen K. Chilamkurti, and Ce-Kuen Shieh. A novel pause count backoff algorithm for channel access in IEEE 802.11 based wireless LANs. In *Proceedings of the International Symposium on Computer Science and its Applications*, CSA '08, pages 163–168, Washington, DC, USA, 2008. (Cited on page 94.)

[128] L. Romdhani, Qiang Ni, and T. Turletti. Adaptive EDCF: enhanced service differentiation for IEEE 802.11 wireless ad-hoc networks. In *IEEE WCNC 2003*, volume 2, pages 1373 –1378 vol.2, march 2003. (Cited on page 94.)

[129] Younggoo Kwon, Yuguang Fang, and Haniph Latchman. A novel MAC protocol with fast collision resolution for wireless lans. In *IEEE Infocom*, pages 793–807, 2003. (Cited on page 94.)

[130] S. J. Golestani. A self-clocked fair queueing scheme for broadband applications. In *Proceedings IEEE INFOCOM '94*, pages 636–646 vol.2, 1994. (Cited on page 94.)

[131] Nitin H. Vaidya, Paramvir Bahl, and Seema Gupta. Distributed fair scheduling in a wireless LAN. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 167–178, New York, NY, USA, 2000. (Cited on page 94.)

[132] Haiyun Luo, Songwu Lu, and Vaduvur Bharghavan. A new model for packet scheduling in multihop wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 76–86, New York, NY, USA, 2000. (Cited on page 94.)

[133] Haiyun Luo and Songwu Lu. A topology-independent fair queueing model in ad hoc wireless networks. In *Proceedings of the 2000 International Conference on Network Protocols*, ICNP '00, Washington, DC, USA, 2000. (Cited on page 94.)

[134] H. Luo, P. Medvedev, J. Cheng, and S. Lu. A self-coordinating approach to distributed fair queueing in ad hoc wireless networks. In *Proceedings INFOCOM '01*, volume 3, pages 1370 –1379 vol.3, 2001. (Cited on page 94.)

[135] W. Pattara-Aukom, S. Banerjee, and P. Krishnamurthy. Starvation prevention and quality of service in wireless LANs. In *The 5th International Symposium on Wireless Personal Multimedia Communications, 2002.*, volume 3, pages 1078 – 1082, oct. 2002. (Cited on page 94.)

[136] Jeng Farn Lee, Wanjiun Liao, and Meng Chang Chen. Inter-frame space (IFS)-based distributed fair queuing in IEEE 802.11 WLANs. In *2nd International Conference on Broadband Networks, BroadNets 2005.*, pages 682 – 689, oct. 2005. (Cited on page 94.)

[137] Jain-Shing Liu and Chun-Hung Richard Lin. Achieving efficiency channel utilization and weighted fairness in IEEE 802.11 WLANs with a p-persistent enhanced DCF. In *Proceedings of the 3rd international conference on Mobile ad-hoc and sensor networks*, MSN'07, pages 174–184, Berlin, Heidelberg, 2007. (Cited on page 94.)

[138] Zakhia G. Abichar and J. Morris Chang. CONTI: constant-time contention resolution for WLAN access. In *Proceedings of the 4th IFIP-TC6 international conference on Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communication Systems*, NETWORKING'05, pages 358–369, Berlin, Heidelberg, 2005. (Cited on page 94.)

[139] Bosheng Zhou, Alan Marshall, and Tsung-Han Lee. A k-round elimination contention scheme for wlans. *IEEE Transactions on Mobile Computing*, 6(11):1218–1244, November 2007. (Cited on page 95.)

[140] Bosheng Zhou and Alan Marshall. A distributed contention vector division multiple access (D-CVDMA) protocol for wireless networks. *IEEE Transactions on Mobile Computing*, 9(7):1049–1054, July 2010. (Cited on page 95.)

[141] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition)*, pages 1 –189, 2005. (Cited on page 95.)

List of Figures

List of Abbreviations

ACK	Acknowledgment
ARUBE	Adaptive Ranking-based Uncorrelated Bit Extraction
BEB	Binary Exponential Backoff
BER	Bit Error Rate
BGR	Bit Generation Rate
CA	Certification Authority
CBR	Constant Bit Rate
CCA	Clear Channel Assessment
CIR	Channel Impulse Response
CQA	Channel Quantization Alternating
CQG	Channel Quantization with Guardband
CRP	Contention Resolution Period
CRT	Chinese Remainder Theorem
CSI	Channel State Information
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
DCF	Distributed Coordination Function
DIFS	Distributed Inter Frame Space
DoS	Denial of Service
ECC	Error Correcting Code
EIED	Exponential Increase Exponential Decrease
EIFS	Extended Inter-Frame Space

ESPAR	Electronically Steerable Parasitic Array Radiator
FDD	Frequency Division Duplex
FFT	Fast Fourier Transform
FIPS	Federal Information Processing Standard
GTW	Grant Transmission Window
HRUBE	High Rate Uncorrelated Bit Extraction
IFFT	Inverse Fast Fourier Transform
KLT	Karhunen-Loéve transform
LDPC	Low Density Parity Check Code
LLR	Log Likelihood Ratio
LOS	Line-Of-Sight
MAC	Medium Access Control
MILD	Multiplicative Increase Linear Decrease
MIMO	Multiple Input Multiple Output
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
OGA	Orthogonal Greedy Algorithm
OTC	Overheard Transmissions Counter
PID	Proportional-Integral-Derivative
PKI	Public Key Infrastructure
QoS	Quality of Service
RBC	Random Backoff Control
rms	root mean square
RSSI	Received Signal Strength Indicator
RTS	Request To Send

SCFQ	Self-Clocked Fair Queuing
SIFS	Short InterFrame Space
SODCA	Self-Organized Channel Access
SPRT	Sequential Probability Ratio Test
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TI	Turn Indicator
TNR	Tap-to-Noise power Ratio
USRP	Universal Software Radio Peripheral
UWB	Ultra Wide Band
WEP	Wireless Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access

Youssef El Hajj Shehadeh

Personal Information

Birthday: November 5, 1986
Birth place: Chehim, Lebanon
Marital status: Single
Address: Christophorusweg.12- App.129, 37075 Göttingen
Email: youssef.hc@gmail.com
Mobile: +49 (0) 152/56185792

Education

2010 – 2013 **Georg-August Universität Göttingen** *Germany*
PhD candidate at the Institute of Applied Computer Science, Telematics Group

2008 – 2009 **Ecole Nationale Supérieure des Télécommunications, ENST Paris (Telecom ParisTech)** *France*
Degree: Master of Research. Major: Digital Telecommunication Systems (Grade: Very Good, 1st Rank)

2004 - 2009 **Lebanese University of Beirut, Faculty of Engineering** *Lebanon*
Degree: Diploma in Telecommunications engineering. (Grade: Very Good, 1st Rank)

2003- 2004 **Lycée Nationale, Beirut** *Lebanon*
Lebanese Baccalaureate- Major: General Sciences. (Grade: Very Good)

Awards

2010 – 2013 **DAAD scholarship:** 3 years PhD scholarship from the German Academic Exchange Service (DAAD).

2008 - 2009 **Bourse Master Ile-de-France:** Master scholarship for Paris region, France.

Experience

03– 09/2009 ***SEQUANS Communications, La Défense, Paris*** *France*
Internship, **"Advanced Channel Estimation Methods at High Mobility in LTE Systems"**

- Study of LTE specifications.
- Investigation of channel estimation performance at high mobility.
- Development and simulation of an advanced channel estimation method.
- Outcome: 3 conference publications, **1 Patent**.

07 – 09/2008 ***OGERO Telecom (operator of PSTN in Lebanon), Beirut*** *Lebanon*
Internship, **"Microwave Transmission"**

- Operation, configuration and troubleshooting of digital microwave systems.

07 – 09/2007 ***Electronic Production & Consulting CO, Beirut*** *Lebanon*
Internship, **"Realization and troubleshooting of electronic platforms and circuits"**

Projects:

- Synthetic study of LTE.
- Study of Multimedia Broadcast and Multicast Services (MBMS) within UMTS.
- Analysis of transmission in GSM using TEMS.
- Study of the physical layer of WIMAX.
- Simulation using NS-2 of TCP congestion control mechanisms.
- Simulation by Java of different waiting list and cache policies of a Web Pool Server.

Teaching:

- Lecture: Security and Cooperation in Wireless Networks, WS 2012/2013.
- Seminar on Network Security and Privacy (NSP): SS 2011; WS 2011/2012; SS 2012.
- Post-Graduate Seminar: WS 2011/2012; SS 2012; WS 2012/2013.

** SS: Summer Semester; WS: Winter Semester.*

Skills

Telecom

- Wireless networks: Physical-layer & MAC layer security, advanced medium access schemes, etc.
- Mobile networks: GSM, GPRS /EDGE, UMTS, HSDPA/HSUPA, HSPA+, LTE
- Transmission techniques: MIMO, OFDMA, CDMA, FDM, TDM, SC-FDMA, etc.
- Digital communications: Coding, modulation, ADC, DAC, decoders, estimation, equalization, etc.

Software

- Software: OMNeT++, MATLAB, TEMS, LabView, AutoCAD 2008, MS/Open Office, LATEX
- Programming: C/C++, Assembly, Java (Basic notions)

Languages

English (Fluent) – **German** (Very Good, level B2) – **French** (Very Good) – **Arabic** (Mother tongue)

Patent

- **Youssef El Hajj Shehadeh**, and Serdar Sezginer, “Method for estimating a received signal and corresponding device”. Granted Patent No. US20110128842, June 2011.

Publications

- **Youssef El Hajj Shehadeh**, Mohamad Hotait, Kifah Tout & Dieter Hogrefe, “Random Backoff Control to Thwart Malicious Behavior in WLANs,” *in the 19th IEEE International Workshop on Local and Metropolitan Area Networks*, Brussels, Belgium, April 2013.

- **Youssef El Hajj Shehadeh**, Omar Alfandi & Dieter Hogrefe, “Towards Robust Key Extraction from Multipath Wireless Channels,” *Journal of Communications and Networks- Special Issue on Physical-layer Security*, Vol. 14, No. 4, pp.385-395, August 2012.

- **Youssef El Hajj Shehadeh**, Omar Alfandi & Dieter Hogrefe, “On Improving the Robustness of Physical-layer Key Extraction Mechanisms against Delay and Mobility,” *in the 8th International Wireless Communications and Mobile Computing Conference*, Limassol, Cyprus, August 2012.

- **Youssef El Hajj Shehadeh**, Ammar El Falou, and Dieter Hogrefe, “On Enhancing the Reliability of Key Extraction Mechanisms from Wireless Channels,*”* extended Abstract, *Pilates’12,* Kaiserslautern, Germany, March 2012.

- **Youssef El Hajj Shehadeh**, Omar Alfandi, and Dieter Hogrefe, “Intelligent mechanisms for key generation from multipath wireless channels,*” in the Wireless Telecommunication Symposium 2011*(*WTS’11),* New York, USA, 13-15 April 2011.

- **Youssef El Hajj Shehadeh** and Dieter Hogrefe, “An optimal guard-intervals based mechanism for key generation from multipath wireless channels,” i*n the 4th IEEE International Conference on New Technologies, Mobility and Security (NTMS 11),* Paris, France, February 2011.

- **Youssef El Hajj Shehadeh**, and Serdar Sezginer, “Fast Varying channel estimation in downlink LTE systems”, *in Proc. PIMRC’10*, Istanbul, Sept. 2010.

- Guillaume Vivier, Serdar Sezginer, Onur Oguz**, Youssef El Hajj Shehadeh**, “Challenges and solutions for high speed channel estimation of IMT.ADV systems**,**” *in Proceedings of Future Network Summit 2010*, Florence, Italy, 16 -18 June 2010.

- **Youssef El Hajj Shehadeh**, and Serdar Sezginer, “An iterative estimator for fast varying channels using successive OFDM symbols,” *in Proc.PIMRC’09*, Tokyo, Sept. 2009.

Göttingen, 15.04.2013