Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access

Project no. 671704
Research and Innovation Action
Co-funded by the Horizon 2020 Framework Programme of the European Union

Call identifier: H2020-ICT-2014-1
Topic: ICT-14-2014 - Advanced 5G Network Infrastructure for the Future Internet
Start date of project: July 1st, 2015

Deliverable D2.6

Role of impairments when using physical layer security

Due date: 31/12/2017
Submission date: 30/12/2017
Deliverable leader: UEssex

Dissemination Level

PU: Public
PP: Restricted to other programme participants (including the Commission Services)
RE: Restricted to a group specified by the consortium (including the Commission Services)
CO: Confidential, only for members of the consortium (including the Commission Services)
## List of Contributors

<table>
<thead>
<tr>
<th>Participant</th>
<th>Short Name</th>
<th>Contributor</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Essex</td>
<td>UEssex</td>
<td>Felix Ngobigha, Mike Parker, Stuart Walker</td>
</tr>
<tr>
<td>Heinrich Hertz Institut, Berlin</td>
<td>HHI</td>
<td>Kai Habel, Volker Jungnickel</td>
</tr>
</tbody>
</table>
# Table of Contents

List of Contributors .......................................................................................................................... 2

1. Introduction ...................................................................................................................................... 6

2. Physical layer security & impairments in multi-user wireless networking ................................. 8
   2.1. Security issues in wireless communications ............................................................................. 8
   2.1.1. Security threats in wireless channel .................................................................................... 9
   2.1.2. Physical layer security in wireless networking ................................................................. 10
   2.2. Physical layer security exploiting channel randomness ....................................................... 11
   2.2.1. Channel Randomness ....................................................................................................... 11
   2.2.2. Threat models in wireless networking ................................................................................ 12
   2.3. Key generation techniques when using PLS in wireless networks ....................................... 12
   2.3.1. Channel State Information (CSI) approach ..................................................................... 13

3. Security & impairment issues in optical networking ................................................................. 17
   3.1. LED-based optical wireless communication ......................................................................... 17
   3.2. Laser-based optical wireless communication ....................................................................... 18
   3.3. Laser-based optical wireline communications ..................................................................... 19
   3.3.1. Introduction to the tapping scenario ................................................................................... 19
   3.3.2. Tap coupler ....................................................................................................................... 20
   3.3.3. Physical Layer Security considering Bob’s SNR advantage ............................................. 25

4. Conclusions .................................................................................................................................... 29

References .......................................................................................................................................... 30

Acronyms ........................................................................................................................................... 33
List of Figures

Figure 1: LED based optical wireless link setup (block diagram) / optical transceiver installed ........................................ 17
Figure 2: Dependence of link performance on weather event for LED based optical wireless link in Berlin (top: SNR/green, rate/orange, bottom: visibility/violet) ........................................................................................................ 18
Figure 3: Block diagram for laser based optical wireless link using the turbulent channel for symmetric key generation [36]........................................................................................................................................... 19
Figure 4: Tap scenario for PON system (only downstream shown) ........................................................................................................ 20
Figure 5: Bend coupler to tap light from a glass fibre (source: Wikipedia) ................................................................................. 21
Figure 6: Bidirectional coupler model........................................................................................................................................... 21
Figure 7: Wavelength allocation plan for different PON systems from APON (1998) to NG-PON2 (2014) .................... 22
Figure 8: Tap coupler properties in dependence of wavelength (optimized for 1500 nm) ................................................................. 23
Figure 9: Tap coupler properties in dependence of wavelength (optimized for 1300 nm) ................................................................. 24
Figure 10: Tap coupler properties in dependence of wavelength (optimized for 1530 – 1600 nm) ................................. 25
Figure 11: SNR advantage model (source: SENDATE project) ................................................................................................. 26
Figure 12: Vulnerable sections in PON downstream ........................................................................................................... 27
Figure 13: Vulnerable sections in PON upstream ..................................................................................................................... 27
Figure 14: Tap coupler properties in dependence of wavelength (optimized for 1680 nm) ............................................................. 27
Executive Summary

This CHARISMA deliverable D2.6 discusses the role of impairments when using physical layer security. Both wireless and wired 5G networking technologies are discussed, including radio frequency (RF) and millimetre wave (mmW) frequencies, as well as optical wireless LED-based and laser-based communications systems. The physical layer principles of how symmetric random keys can be generated by exploiting the shared randomness of multi-path channels are explained, as is how channel reciprocity and maximal entropy (based upon privacy amplification) can be utilised to generate strong keys. Here, channel state information (CSI) using uncorrelated channel phase, received signal strength, and quantisation, for key generation is also discussed.

The PHY layer security issues of optical fibre-based wireline technologies are also presented, based upon passive optical networking (PON) topologies, and particularly the 100G OFDM-PON system that has been developed within CHARISMA. In particular the issues of coupling ratios, power levels, and wavelength allocations when an eavesdropper employs a tapping coupler to evanescently leak optical signals from the optical fibre are discussed. In addition, the danger of the SNR advantage model featuring a “security gap” is presented, and the application of punctured LDPC codes to mitigate against such an attack is described. A quantitative power budget table is also presented for the 100G OFDM-PON architecture, to show the impact of power levels on physical layer security.
1. Introduction

In this CHARISMA deliverable D2.6 “Role of impairments when using physical layer security”, we describe how the physical properties of future 5G networks (both wireless, as well as the fixed or wireline segments) can play a role in their security safeguarding, but also in the physical layer impairments that can cause weaknesses in the overall security integrity of the 5G network, and which therefore need to be mitigated against. Future 5G networks are expected to feature numerous sensors and actuators i.e. massive Internet of Things, mIoT, deployment, often for mission critical applications (e.g. intelligent transport systems, ITS) such as driverless cars, ultra high-speed trains, emergency situations (Critical Communications, CriC), and Big Events, such that along with the very high quantities of data that 5G networks will be transporting, the issue of security is of ever increasing importance. Some of these use-cases feature in the field-trial demonstrators of the CHARISMA project (see the deliverables D4.2 and D4.3 of the work package WP4), although the physical layer security (PLS) aspects of this deliverable D2.6 do not themselves feature in the final demos of the project. Rather, this deliverable discusses the different physical layer principles associated with wireless and wireline 5G communications, with a theoretical analysis of the impact of physical layer impairment effects on the security performance of 5G networking. Within the constraints of the CHARISMA project, security has been implemented at the higher layers of the stack, i.e. as exemplified by its end-to-end virtualised security design, as described in the earlier deliverable D2.5 “CHARISMA e2e v-security architecture”. As such, the work presented in this report represents a more fundamental research approach that has not been incorporated into the final CHARISMA architecture, but provides a theoretical understanding of the PHY security issues confronting 5G networking. However, being a PLS approach, the results presented here are therefore highly complementary to the virtualised and higher-layer security solutions of workpackage WP3, and so are not intrinsically excluded from future implementation.

When considering the wireless domain, this aspect of 5G networking includes radio, millimetre wave (mmW), and free-space optical frequencies, all of which feature in the PLS techniques discussed in this deliverable. In addition, the 5G wireline networking aspects are also represented by the 100G OFDM-PON technology that features in the CHARISMA architecture, and which also presents its own PLS features that are discussed here.

Particular physical layer impairments considered in this D2.6 report, include the effects of noise, path loss, shadowing, multi-path interference, and fading in the wireless domain. In the wireline (i.e. optical fibre) domain, the key PLS issue is that of tapping of evanescent light from a single mode fibre (SMF) link for eavesdropping purposes. This latter aspect causes signal power reductions, and when large enough, will be noticed by the passive optical networking (PON) monitoring system. Such evanescent tapping also features wavelength effects (i.e. chromatic and polarisation dependencies), which also therefore need to be taken into account.

Public and private key generation, particularly using symmetric secret keys, are an important aspect of safeguarding 5G networks, both over wired and wireless channels. In particular, for channels with randomly varying physical layer characteristics, the entropy associated with such links can be exploited as a means to create symmetric secret keys between transmitting and receiving nodes. Channel reciprocity allows the generation of symmetric keys, and a common feature of the physical layer is that of relatively slowly-changing physical properties, such that from a practical point of view the channel can be assumed to be reciprocal; indeed for electro-magnetic (EM) radiation (i.e. all of radio, mmW, visible and infra-red light, comprising the EM spectrum) reciprocity can generally be guaranteed as long as there are no magnetic sources or influences.
Indeed, simple absorption/attenuation (lossy) elements, as well as linear effects such as chromatic and polarisation dispersion can be represented by appropriate Hermitian transfer matrices, which are intrinsically reciprocal in nature. In which case, the generation of symmetric random keys in wireless and wired networks by exploiting the randomness of multi-path channels is a reasonable and practical proposition.

This deliverable D2.6 is organised as follows. In Chapter 2 we discuss the impact of physical layer impairments on wireless PLS, with particular regard to the issues of integrity, confidentiality, availability, and authentication in wireless networking. The security threats in a wireless channel of passive and active attacks (including denial of service, DoS) are presented, and a discussion of how public key infrastructure (PKI) mechanisms in the context of a certification authority (CA) can be employed to mitigate these threats. The inherent randomness of multi-path fading channels is then discussed, so that key generation using channel state information (CSI), including uncorrelated aspects of channel phase, received signal strength, and quantisation as a means to maximise available entropy (i.e. using privacy amplification) for key generation is described. Chapter 3 discusses the security and impairment issues in optical networking, with regard to LED- and laser-based optical wireless communications, and then on to PON fibre-optical based (i.e. wired) infrastructures. Here, the issues of evanescent tapping (i.e. a tap coupler) are discussed, focusing on the coupling ratio that an eavesdropper might employ, and the wavelength (i.e. chromatic) dependencies that such power leakage might exhibit. In particular, the danger of the signal-to-noise ratio (SNR) advantage model is also discussed, with special regard to the “security gap” than can occur if a suboptimum low-density parity check (LDPC) code is employed between the transmitting and receiving nodes. The implications of this on the 100G OFDM-PON backhaul link are quantitatively analysed via a full power budget analysis. Finally, chapter 4 presents some concluding remarks.
2. Physical layer security & impairments in multi-user wireless networking

In the CHARISMA architecture, there are various wireless and wireline links, e.g. between the end-users (or user equipments) and the CAL0, and between CAL0 and CAL1, which may use RF, millimetre wave (mmW) or optical wireless connections; or the backhaul between CAL2 and CAL3 which is connected using an optical fibre, e.g. the 100G OFDM-PON technology, and also as can also be found in the general topology of a C-RAN infrastructure. In wireless communication systems, the physical medium corresponds to the free-space in which the electromagnetic wave propagates. As in any telecommunications system, the wireless signals are subject to corruption by the inevitable presence of impairments such as noise at the transmission and reception ends, as well as along the transmission medium. Apart from the hardware based electronic noise (such as thermal noise) corrupting the signal, certain characteristics of electromagnetic (EM) wave propagation in the wireless environment can also impair the signals under transmission. Such impairments arise from signal fading and shadowing effects due to scattering, reflection, and refraction, that the electromagnetic wave may face during propagation, as well as attenuation of the EM energy as a result of absorption due to rain, snow etc. The role of these impairments when applying physical layer security (PLS) in the wireless domain could significantly influence the received signal levels. As a mobile unit traverses its path, the propagation characteristics and interference effects can change dynamically due to the mobility involved, while the traditional higher-network-layers [1, 2] of providing wireless network security (cryptography) can be complex and difficult without the necessary infrastructure; i.e. appropriate studies are therefore also appropriate to consider PLS in modern wireless communication systems. Indeed, these characteristics of impairments are not necessarily disadvantageous when using physical layer security due to the randomness of the wireless channel [3, 4, 5, 6, 7]. When properly explored, these impairments can permit very efficient spectrum utilization, and can also increase the security of communication transmissions as a result of the noise [8]. The study reported in this deliverable is intended to describe the potentially important role of impairments in wireless communication systems such as the wireless segments of the CHARISMA architecture, with particular interest on readily available solutions in terms of PLS, which to now has still been largely seen as a theoretical issue [6].

2.1. Security issues in wireless communications

Recently, different approaches to security have emerged from the area of information theory under the generic term physical layer security. In the wireless domain, PLS is assumed to encompass all keyless security technologies that can ensure perfect secrecy by exploiting a source of entropy typically considered a foe rather than a friend; that is, the noise and interference in real communications media. PLS was pioneered by Wyner [8], and is founded upon the theoretical basis of the Shannon noiseless model [9]. It can be presumed that in all realistic communications settings between a source node (commonly denoted as “Alice”) and an intended destination node (commonly referred as “Bob”), the observation of Bob and an adversary (commonly denoted as “Eve”) are different realizations of a joint probability distribution, i.e. the output of the channel transmission. In wireless communications, the modes of operation across the transmission medium consist of two main aspects: Broadcasting and Superposition [10]. Both these features possess characteristics that pose a challenge.
to achieving reliable and secure communications between a transmitter and receiver in the presence of an adversary. For example, due to the broadcast nature of the wireless channel, shielding of the transmitted signal from an unintended receiver is a difficult task, thus making the channel vulnerable to eavesdropping, message modification, node impersonation and other kinds of attacks. In this study, some important features of secure wireless network as given in [11] are of particular relevance:

- **Integrity:** This stand for the soundness of the message data arriving at the destination nodes. Secure and reliable transmission requires that the message received by the legitimate note should not have been tampered with or altered in any form by an adversary. Thus the message data sent over the wireless channel should maintain their integrity even when an adversary has tried to intercept and modify it.

- **Confidentiality:** This requires that the privacy of the transmitted message data be maintained even in the presence of an eavesdropper. Unauthorized nodes should not have access to the message transmitted.

- **Availability:** This property requires that the network should be absolutely functional under any circumstance when legitimate nodes require its service. To this end, the system should not be susceptible to any form of attack posed by the adversary when the legitimate nodes are communicating over the system.

- **Authentication:** This requires that only legitimate nodes are able to communicate with each other and that they do not communicate with illegitimate nodes, therefore maintaining the confidentiality of the system. In essence, authentication ensures that all nodes attempting to communicate are in fact legitimate nodes. Thus verification of the identity of the communicating nodes is necessary.

### 2.1.1. Security threats in wireless channel

The discussion of threats in wireless networking is often organised into passive and active attacks. In the former, the attacker remains unnoticed in the background while carrying out his attack. He does not disrupt the normal operation and functionality of the routing protocol of the network, unlike an active attacker. The properties of these two attacks are detailed below [11, 12]:

**Passive attack**

In a passive attack, an adversary (e.g. located between the end-user and the base station at CAL0) silently steals data exchanged over the wireless network without the operation of communication being impeded, and is summarized as below:

- **Eavesdropping:** An adversary intercepts, and reads messages and conversations that were intended for a legitimate receiver;

- **Traffic Analysis:** An adversary who cannot eavesdrop and read the communication between two nodes can still gain routing information, with which he can subsequently determine the location and identities of the communicating parties by analysing their communications patterns;
• Node Impersonation and routing attack: Here, the nature of this attack is such that, an adversary attempts to camouflage himself as an idle node within the wireless network, so as to deceive a legitimate node into thinking that he is another legitimate node, and thus be able to steal valuable information transmitted over the network.

**Active attack**

In this type of attack, the adversary actively attempts to disrupt the normal operation of the network, e.g. at the various intermediate CALs (CAL0, CAL1, CAL2) with the goals of such an active attacker summarized below:

- Denial of service attack: Denial of service (DoS) can either be as a result of a network failure or a malicious adversary trying to disrupt communication. The classical way of carrying out this attack is that of jamming of signals and battery exhaustion. The threat is severe if the adversary has enough computing power and bandwidth, as this can generate a signal strong enough to overwhelm the targeted signal and interrupt communications. This example, as well as the distributed DoS (DDoS) version, is the subject of the CHARISMA lab demonstrator at Demokritos in Athens (see the associated deliverables D4.2 and D4.3).

- Attack against routing: In this attack, the adversary intercepts a routing packet, modifies its content and transmits it back into the network. The attacker can also choose to transmit the intercepted original packet, but at different times, thus sending outdated routing information to the legitimate nodes. The purpose of these attacks is to deceive the routing nodes with conflicting information, delaying packets, or preventing them from reaching their destination node. It is therefore apparent that an active attack can subvert the integrity of the routing protocol by modifying it, therefore fabricating false routing information, which is sent back into the nodes. To carry out these attacks, the adversary must be able to intercept and inject packets into the network.

2.1.2. Physical layer security in wireless networking

As discussed in [11], the conventional approach to security in wireless networks involves the use of secure protocols at the higher layers (i.e. application layers), which are based on cryptographic algorithms and a shared key, to scramble the transmitted data between a pair of communicating nodes. Cryptographic algorithms used in wireless communication are based on the argument that it is computationally infeasible to decipher scrambled data without knowledge of the shared key. These cryptographic algorithms require key establishment (key generation and agreement) between two users in a secure manner. An important aspect of security in wireless communication, particularly in 5G networks such as CHARISMA, is the distribution of the secret key between the communication nodes. A traditional solution employs a public key infrastructure (PKI) mechanism for key exchange in the presence of a certification authority (CA). A classical example of such PKI is the Diffie Hellman (D-H) algorithm [13], which is used to derive symmetric keys over an unsecured channel. As such, a PKI mechanism algorithm is only computationally secure, in that it requires a high computational complexity. For example, the D-H algorithm requires fast exponentiation, which can be a difficult operation for mobile devices. Also, the need of a CA further makes these solutions impracticable in some scenarios, such as in sensor and ad-hoc networks [14].
2.2. Physical layer security exploiting channel randomness

Wireless channels are usually modelled as multipath fading channels, e.g. as experienced by RF or mmW links between end-users and a base station located at CAL0. Here, a multipath fading channel is assumed that a transmitted signal over the channel propagates through the wireless channel experiencing reflection, diffraction and scattering from objects between and around the transceiver, and arrives at the receiver via several paths. The signal at the receiver is therefore a summation of the signals over the multiple paths, which have different amplitudes and delays [15]. Thus a multipath fading channel can be modelled as a combination of different channel impulses having different amplitudes and delays.

Due to the relative movement of the communicating nodes and that of the reflecting clusters, the paths change randomly causing the channel to vary with time, thus producing random fluctuation in the phase and amplitude of the received signal. The random variation of the channel properties due to the multipath fading gives rise to four properties, which are considered the foundation of physical layer security in wireless communications [15], and which are described below.

2.2.1. Channel Randomness

The fading of the channel is random over time due to spatial selectivity of the multipath propagation, with the channel state also being random over frequency due to the frequency selectivity of the multipath channel.

- Temporal Variation: Here the channel fading varies randomly with time due to multipath propagation, which arises from the mobility of the communicating nodes and objects in the environment near the nodes. An important parameter to consider is the coherence time. The coherence time is a statistical measure of the time duration over which the impulse response of the channel is static. It is also employed to measure the similarity of the impulse response of the channel at different times. Due to multipath propagation, the channel fading measured at several time instants is random and independent of each other if the interval between the measurement times instant is greater than the coherence time of the channel.

- Frequency Selectivity: In a multipath propagation, each possible path is affected by different attenuations and delays, with the received signal consisting of a combination of all signal paths by wave interference. A variation in the carrier frequency (phase) of the transmitted signal results in a random variation of the signal strength even when the signal paths are unchanged [16].

- Spatial Variation: A major security parameter, which is based on the well-known Jakes uniform scattering model [17], is the coherence length of the channel, which is the distance after which the channel correlation goes to zero. A received signal rapidly decorrelates over a distance of roughly half a wavelength, such that a spatial separation of one or two wavelength is sufficient to assume independent fading channel paths. This implies that, a node (Eve), which is at least half a wavelength from two other communicating network nodes (Alice and Bob) experiences a channel fading which is statistically independent of the fading channel between the two communication nodes (Alice and Bob). Thus the properties of a wireless channel are unique to the locations of the two communicating nodes (Alice and Bob) [18].

- Channel Reciprocity: Two nodes communicating within the coherence time of a channel experience the same channel fading. Thus the multipath properties of the wireless channel are identical in both directions of the
channel link. The principle of channel reciprocity plays a key role in key establishment in physical layer security [19].

2.2.2. Threat models in wireless networking

The attack model for a wireless communication system consisting of three nodes is presented. Alice and Bob are legitimate nodes (e.g. in the CHARISMA context this could be CAL0 and an end-user, respectively) who want to communicate securely. Eve is a potential eavesdropper. Alice has a transmitter with $N_T$ transmit antennas, which transmit data to Bob with $N_R$ receive antennas in the presence of the adversary Eve with $N_E$ eavesdropping antennas. The adversary model for the physical layer security schemes is summarized below:

- A passive adversary, Eve, can listen to all communications between Alice and Bob. This is due to the broadcast nature of the wireless channel.

- Eve’s aim is to derive the shared secret key between Alice and Bob, and not to disrupt the key establishment procedure by jamming the communication between the legitimate nodes. Eve cannot modify information transmitted over the wireless channel by Alice and Bob [20].

- Eve can measure the channel property between herself and the two communicating nodes (Alice and Bob). Eve obtains information on the channel between herself and the legitimate nodes by exploiting the channel estimation procedure carried out by Alice and Bob. In order to exploit the common randomness offered by the time/frequency variant fading channel between the two nodes, and the multiplexing gain provided by the use of multiple antennas for key establishment, the legitimate nodes must estimate the channel between them. The channel estimation involves Alice sending probe signals from each of her $N_T$ transmit antennas to each of Bob’s $N_R$ receive antennas, and vice-versa. Using the probe signal, they both estimate their channel. It is important to note that Eve is capable of eavesdropping on the probe signals exchanged between Alice and Bob, so as to estimate the channel between her and the legitimate nodes [21], thus allowing her to derive some pattern only known to her. This is a common attack system where the secret key is extracted from the received strength of the signal. When the two legitimate communicating nodes are immobile, the wireless channel between them is relatively stable. The adversary Eve can then employ predetermined movement patterns, thus creating a desired and predictable change in the channel measurement between the two nodes. In practice, this occurs when Eve blocks the line of sight between Alice and Bob by crossing the link between them, causing the transmitted signal between them to experience sharp attenuation. This type of attack is known as a Predictable Channel Attack [22].

- Eve is assumed to have a full knowledge of the key extraction algorithm and the full parameters.

2.3. Key generation techniques when using PLS in wireless networks

Physical layer based key generation exploits the common randomness such as noise and interference within a channel to establish secret keys. The common randomness is exploited from the properties of the wireless channel, e.g. a mmW, RF, or optical communications link in the CHARISMA network. A common practice is to extract the shared randomness from the phase or the amplitude of the received signal, e.g. particularly in the
RF and mmW cases. In general the key generation process consists of collecting the channel state information (CSI), such as channel quantization and key agreement, information reconciliation and privacy amplification.

2.3.1. Channel State Information (CSI) approach

In order for the communicating nodes to generate a secret key, they must be able to acquire the channel state information (CSI) [11] of the wireless channel. In order for two nodes, Alice and Bob, to estimate the CSI of the wireless channel between them, they first have to exchange known probe signals (pilot symbols) via the wireless channel [23]. This is so that Alice, within the first time slot, transmits her probe signal to Bob. Bob, upon receiving this, measures the value of the received probe signal and extracts the CSI from it. In the second time slot, Bob then transmits his probe signal to Alice.

It is imperative for Alice and Bob to perform the channel estimation as fast as possible, so as to avoid any decorrelation between the CSI, which they have estimated. A common practice is to make the length of the time slot to be half of that of the channel coherence time. Eve also tries to derive an estimate of the CSI of the channel between herself and Alice/Bob. However, her observation of the CSI is independent of Alice and Bob’s observation due to the time varying multipath fading of the wireless channel. A variety of CSI information [11] can be used, including the channel impulse response, received signal strength indicator (RSSI), signal envelope, and signal phase.

Received Signal Strength

The received signal strength (RSS) is a measurement of the power present in the received signal. Using the RSS as the CSI has received a lot of attention over the years due to the ease of extracting the RSS from commercial-off-the-shelf wireless cards [24]. Previous studies [25] on RSS based methods were focussed on exploiting the temporal variation, spatial variation and frequency selectivity of the wireless channel. Other studies were directed towards exploiting multi-antenna diversity for extracting the shared randomness and generating secret keys. However, using RSS provides a coarse grained CSI, thus it suffers from a low key bit rate. In [26] Mathur proposed a level crossing based key extraction algorithm. The algorithm starts by Alice and Bob alternatively probing the channel between them, so as to collect a relatively large block of consecutive channel estimates (i.e. measure the RSS). Jana in [27] proposed an Adaptive Secret Bit Generation (ASBG), which is a modified version of that proposed by Mathur. Her method incorporates two well-known information reconciliation and privacy amplification methods. The RSS being provided by single channel estimation is therefore coarse grained, thus it does not provide enough entropy for a symmetric key. Multiple input multiple output (MIMO) systems have received a lot of attention over the years as reported in [24]. This has brought about the concept of exploiting the available spatial dimension to enhance the secrecy capacity of a wireless channel. Generally, a fading MIMO channel means that the transmitter, receiver and adversary need to be equipped with multiple antennas respectively.

Zeng in [23] demonstrated the multiple antenna diversity of a MIMO system by measuring the RSS value between each antenna pair in round-robin way. Here Alice and Bob were equipped with three antennas each, thus they have nine antenna pairs. The channel probing is performed in a periodic pattern, unlike the previous methods discussed, such that the sub-channels are probed periodically. There are two reasons for this type of probing: (i) each sub-channel has a limited dynamicity, which is constrained by the coherence time of the channel. (ii) A single bidirectional probing can be done much faster than the channel coherence time, thus allowing multiple sub-channels to be probed within the coherence time. Thus, there is potentially enough
flexibility to exploit the multiple antenna diversity by probing different sub-channels in a round robin way. Although using multiple channel estimations over time can provide enough entropy for key generation, it can however contain correlated components, which makes it difficult to verify the security level of the key material. Alternatively, in order to reduce this correlation, another approach is to utilize only a portion of the quantized channel profile by down-sampling the raw CSI measurement in time, and so reduce the strong correlation. However, this is done at the expense of a reduced key generation rate. An alternative approach was also proposed in [19], where the discrete Karhunen Loeve transform was employed in order to convert the measured channel samples into uncorrelated samples.

Secret key generation using the RSS method is practically feasible with the existing wireless platform, however it has a very low key bit-rate, which limits its application due to the intermittent connectivity in mobile environments. In addition, the RSS-based key generation method depends on the channel variation or movement of the nodes to extract a high enough entropy for key generation. The effect of this is that the RSS technique is not suitable for key generation in static environments. Another major limitation of the RSS secret key generation method is that it cannot be extended to support group key generation. The reason for this is that the measured RSS values obtained between communicating nodes cannot be passed securely and efficiently from one node to another, as is required for gathering RSS information across multiple nodes for generating and establishing group keys.

Channel Phase

In [28] the issues associated with the RSS based key generation scheme are resolved with the use of channel phase as the channel state information. The phase reciprocity of the wireless channel between two communication nodes (Alice and Bob) has some major advantages over the RSS method. Unlike the RSS, the channel phase of the received signal has a uniform distribution under a narrow-band fading channel. Current state-of-the-art in signal processing arguably allows for a very high resolution in the phase estimation of the wireless channel, thus allowing for a higher key generation rate when the channel phase is used as the CSI. A major advantage of using channel phase is that the measured channel phase value can be accumulated across multiple nodes.

The earliest report on using channel phase for key generation via exploitation of the channel properties is presented in [28]. In this study, the differential phase between two sinusoids is encoded for key generation purposes. A key generation protocol based on the channel phase for a wideband channel, such as an Orthogonal Frequency Division Multiplexing (OFDM) system, which exploits the inherent randomness of a channel, was proposed in [29]. In an OFDM system a single channel utilizes multiple sub-carriers on adjacent frequencies. Each sub-carrier serves as a source of randomness for key generation, resulting in an increased key generation rate. Using a wideband channel offers a large number of statistically independent degrees of freedom, thus allowing for the generation of large and secure keys. A major contribution is the characterization of a key parameter, which is the probability that two nodes at the end of a wireless channel will generate the same quantization index as a function of the operating signal to interference and noise ratio and the number of quantization levels. Phase estimation is just the channel estimation with probe signal as discussed in the RSS based technique.

As discussed in [11], using the channel phase as a CSI allows for the establishment of a group key, which can be used to improve security in a multicast transmission. Multicast transmission is an efficient method when users
request identical information. Group key generation and distribution without the aid of a key management centre is a difficult task. A group key establishment protocol has been proposed in [30], where the process starts with the communicating node selecting a node to be the master, whose job it is to generate keys among the other nodes, which are the clients. During the group key generation, a client transmits a fixed phase probe signal to the master, with the master then using this to estimate the phase of the channel and then to record it. The master node subsequently selects a probe signal with phase, which is applied identically to all the clients in the group, then evaluates the phase offset. Depending on the phase offset, the master node transmits a probe signal whose phase has been steered using the phase offset to the client. The clients on reception of the probe signal, estimate the steered phase, and quantize it to extract the key information.

When the size of the group increases, the number of interactions between the nodes increases linearly which makes the protocol inefficient for large group sizes. An efficient group key generation using channel phase was presented [31]. In this case, a time slotted round-trip scheme was employed, where group key generation is achieved by first selecting one of the communicating nodes as an initiator. The chosen node starts the generation process by transmitting sinusoidal beacons in both clockwise and counter-clockwise directions. Each node estimates the phase of the sinusoidal beacon in its previous timeslot and generates a periodic extension of the received beacon for transmitting in the next time slot. The absolute phase of the beacon received by a node does not have any phase offset relative to its own local reference time, since all the nodes share a common reference time. Thus it is possible to accumulate the channel phase information along the transmission circuit by periodic extension of the transmitted beacons at each node. Due to the channel reciprocity, the sum of phase estimates across the nodes obtained from clockwise and counter-clockwise transmission, are nearly identical at each node, thus a shared key can be generated.

Quantization

In order for two nodes (Alice & Bob) to communicate securely, they must convert their estimated CSI into identical bit strings by performing quantization on their respective CSIs [11]. This requires the derived key to meet certain constraints described below:

- Suitable Length: The key should have a length of 128 to 512 bits as required in symmetric encryption algorithms.

- Statistically Random: The produced key bits should not suffer from statistical defects, which could be capitalized upon by an adversary. This implies that a generated secret key of length \( N \) must provide \( N \) bits of uncertainty to an adversary who only knows the key generation algorithm.

In a single carrier system, the quantization of the CSI can only be done in the time domain, while for a multi-carrier system like OFDM, secret bits can be extracted from the OFDM sub-carriers in the frequency domain. This is done by quantizing the amplitude of the CSI across several sub-carriers, so as to increase the key generation rate. Many quantization schemes for translating the estimated CSI into a key bit string have been proposed by several authors. Some of these schemes were designed to operate with the phase of the complex channel impulse response, while most schemes proposed in the literature have been designed for systems using RSS as the source of randomness. In this study, the quantization technique can be categorized into two approaches: Lossy [32, 33], and lossless quantization [34].
**Lossless and Lossy quantization methods**

In the lossless quantization, also described as Direct Quantization [34], the CSI is used to create quantized data in order to increase the bit generation rate, and the entropy of the bit stream is increased by amplification. Generally, a quantizer is described as lossless if one bit or more is obtained by quantization of a single CSI sample that is greater than, or equal to, a bit per sample. Although this approach generates a key bit at a high rate, the entropy of the generated key is low. The low entropy of the generated key is compensated for by using privacy amplification to extract a high entropy bit stream from the generated key. It should be noted that using privacy amplification requires a large portion of the bit stream to be removed, so as to extract a bit stream with high entropy; thus the resultant bit rate is reduced.

The lossless quantization method briefly described above is prone to error, as a result of sampling the CSI at border regions. The lossy quantization approach avoids CSI sampling by probabilistically discarding them, so as to maintain a high reliability (key agreement) and entropy. A quantizer based on the median value of the RSS estimate was proposed in [33]. Here, the median value of the measured RSS is used as a threshold, with measurements close to this value being discarded. Basically, this technique has a low key agreement rate and low entropy, thus it is not a good choice for generating secret keys from CSI samples. In [32] quantization based on the differential RSS values is proposed. In this case, the quantizer evaluates the difference in the RSS values and employs two different thresholds to remove the differential values of the RSS estimates, which tend not to be similar. However, just as in the previous quantizer, this approach produces a bit stream with low entropy. Other methods of lossy quantization techniques not mentioned in this study are highlighted in the references [15, 23, 26, 35].
3. Security & impairment issues in optical networking

In this chapter, the security and physical impairment issues with optical wireless as well as optical wireline communications are discussed. First, a LED-based visible light communication link for backhaul applications is described with respect to the inherent security features of the physical layer, with the features of a laser-based point-to-point link also being presented. Finally the security issues of passive optical networking (PON) networks at the physical layer are discussed.

3.1. LED-based optical wireless communication

An LED-based optical wireless link has been installed in Aveiro/Portugal recently in a CHARISMA WP4 activity (e.g. see the deliverable D4.2). The point-to-point link uses an adaptive modulation formats (e.g. DMT) in order to adjust to changing channel conditions in an outdoor environment. It was installed in order to acquire statistical data for bitrate as well as weather data in order to identify conditions, where the link performance is bad or the link fails.

![Figure 1: LED based optical wireless link setup (block diagram) / optical transceiver installed](image)

Due to its physical layer properties, the optical wireless link has a few advantages with respect to its intrinsic security profile as compared to classical RF (point-to-point) wireless links:

1. For optical wireless links, it very easy to collimate and control the light beam by means of lenses or masks. Therefore, the signal leakage to unwanted receivers is smaller, e.g. as compared to RF wireless systems.
2. Optical light can be shielded easily by opaque surfaces. Therefore, an attacker needs to be close to the light beam in order to detect any leaking data. This kind of attack is easier to be noticed as compared to RF wireless, where an attacker can even be outside of a building, or in a nearby room in the same building, and still receive significant amount of RF signal power.
3. Jamming is more complicated in the case of optical wireless systems as compared to their RF wireless counterparts. An attacker would need to have a line-of-sight (LoS) access to the optical receiver in order to blind it. In the case of RF wireless the attacker needs to be close to the receiver, but there is no requirement of a line-of-sight connection.
These inherent physical layer properties make it easier to provide security for an optical wireless link. The link properties, especially the achievable data rate, together with the link signal-to-noise ratio (SNR) depend mainly on the weather parameters, such as the visibility together with amount of precipitation. A weather event and its impact on the link performance is shown in the following Figure 2.

![Figure 2: Dependence of link performance on weather event for LED based optical wireless link in Berlin (top: SNR/green, rate/orange, bottom: visibility/violet)](image)

It can be seen that the visibility decreases to a few 100 m at 5:00am. At the same time the SNR of the link reduces from 32 dB to a value of between 20 - 25 dB. This triggers a reduced data rate (gross) of about 200 Mb/s, down from 450 Mb/s before the event. However, the LED-based optical wireless link is still in operation throughout the event with a useful throughput capacity.

### 3.2. Laser-based optical wireless communication

Although, not forming a central part of the CHARISMA research, laser-based-systems might play a role for 5G installations in the future. Their physical layer properties as compared to LEDs with respect to security are described in this section. LED-based optical wireless links for point-to-point applications are limited to data rates of about a few 100 Mb/s, while bridging up to 200 m distance, laser-based links can provide more available bandwidth and data rates, albeit at the cost of increased complexity. Besides the obvious advantage of an increased data rate, laser-based optical wireless links can also provide increased security.

Compared to LED-based systems, the optical beam of such laser-based systems can be more collimated, so that it is even more difficult for an attacker to acquire signal power as the leakage is reduced further still.
Furthermore, laser-based (or, to be more specific, single mode) point-to-point links can use the channel reciprocity between transmitter and receiver to distribute secret keys and so communicate secretly between the terminals. Such a laser-based system has been proposed in [36].

![Figure 3: Block diagram for laser based optical wireless link using the turbulent channel for symmetric key generation [36]](image)

This approach uses the channel reciprocity between the single-mode transceivers of an optical wireless link, where the atmospheric turbulence modulates (randomly) the phase of the free-space laser beam. The actual key generation principle has been described before in [37]. In this case, the secret signal can only be measured at Alice’s or Bob’s transceiver position, with the secret signal not being available elsewhere by an eavesdropper (e.g., located in a midway path, or next to Alice/Bob etc.). This method of optical wireless link transmission can bridge distances from 500m up to 50km and could be an alternative to wireless point-to-point links for highly aggregated traffic for next-generation mobile networks. A demonstration has shown a transmission of 2x1.7 Tb/s over a link distance of 380 m in 2016 [38].

### 3.3. Laser-based optical wireline communications

#### 3.3.1. Introduction to the tapping scenario

The CHARISMA architecture considers highly aggregated fibre-based backhaul links in order to provide the high data rates of 5G to the mobile access point and end-users. Of particular interest is the OFDM-PON, where a central node, the optical line termination (OLT), can provide up to 100 Gb/s at the physical layer to a set of distributed optical network units (ONUs). Security can be provided at all layers of the protocol stack starting from the physical layer at the bottom up to the application layer.

In this section, the application of security at the physical layer will be discussed using the example of the OFDM-PON, but the results are applicable to PON systems in general. An attacker (Eve) can tap the PON system at the physical layer at different locations. Most promising for an attacker is the link between the OLT and the remote node, the feeder. On that PON section, all down- and up-stream traffic is aggregated and available. The downstream traffic is also available at each branch of the PON; but this not true for the upstream traffic. In Figure 4 are shown the typical PON architecture (downstream only) including Alice and multiple Bobs, together with the possible locations for an attacker, Eve.
In order to acquire the data at the physical layer, Eve would need to have physical access to the transmission fibre itself and would need to couple out parts of the light. In order to perform this action, a bend coupler is required. The difficulty for an attacker is to stay undetected, because physical conservation laws require that any tapped optical power also reduces the optical power for the legitimate receiver Bob. These relations are discussed in the following section.

3.3.2. Tap coupler

In this section, the properties of a tap coupler are discussed in more detail. Such a tapping device is shown in Figure 5. Here, the (yellow) fibre to be tapped is shown in the upper part, while the black mechanical system bends the fibre and attaches an optical system consisting of lenses to couple the evanescent (leaked) light into
a second fibre. Since the tap coupler only performs the coupling/tapping step, the actual receiver can be connected remotely at the far end of the tap fibre.

The tap coupler uses the physical principle of a single mode fibre (SMF), whereby bending of the SMF fibre causes those parts of the light not guided within the fibre core anymore to leak through the cladding out to the outside. In a bending geometry, the outer part of the wavefront sees a longer distance as compared to the distance experienced by inner part of the wavefront. In order for the wavefront to remain in phase, the outer parts of the wavefront would need to travel with a velocity larger than speed of light. Since this is not physically possible, the SMF therefore does not guide those parts of the wavefront anymore and they leak out.

The general properties of an optical coupler can be described using the model given in Figure 6. Here, the loss in the downstream direction is given by $L_{21} = P_2 - P_1$. The coupler ratio in dB is given by $CR = 10 \cdot \log_{10}(T_2/P_1)$, which therefore also describes the relative light power strength (in dB) of $T_2$ relative to $P_1$. The equation for the upstream direction can be derived in a similar manner.

---

1. [Link to Wikipedia](https://de.wikipedia.org/wiki/Abh%C3%B6rger%C3%A4t#/media/File:Biegekoppler_an_einem_Glasfaserkabel_(Coupler-Methode).jpg)
In the following table, the coupling ratio and loss (i.e. leakage power) into the forward direction is given for an ideal optical coupler, i.e. a coupler without excess loss. The output powers at $P_2$ and $T_2$ are also given using an example input power $P_1$ of 1 mW.

Table 3-1: coupler ratio and coupler loss for an ideal optical coupler and example power values

<table>
<thead>
<tr>
<th>Coupler ratio (dB)</th>
<th>Loss (dB)</th>
<th>$P_1$ (mW)</th>
<th>$T_2$ (mW)</th>
<th>$P_2$ (mW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>-3</td>
<td>-3</td>
<td>1</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>-6</td>
<td>-1.2</td>
<td>1</td>
<td>0.25</td>
<td>0.75</td>
</tr>
<tr>
<td>-10</td>
<td>-0.45</td>
<td>1</td>
<td>0.1</td>
<td>0.9</td>
</tr>
<tr>
<td>-15</td>
<td>-0.14</td>
<td>1</td>
<td>0.032</td>
<td>0.97</td>
</tr>
<tr>
<td>-20</td>
<td>-0.044</td>
<td>1</td>
<td>0.01</td>
<td>0.99</td>
</tr>
<tr>
<td>-30</td>
<td>-0.0044</td>
<td>1</td>
<td>0.001</td>
<td>0.999</td>
</tr>
</tbody>
</table>

As stated before, the attacker faces the problem, that any tapping causes a power loss in the forward direction. Since power meters or optical time domain reflectometers (OTDRs) can easily monitor optical fibres, the loss should not exceed 0.2 dB. Even loss events can be found by an OTDR. Therefore, the coupler ratio should be below 13 dB, otherwise the tapping can be easily detected.

Tap couplers have another property, which is important in the PON tapping scenario. The bending loss of the single mode fibre, or the amount of light, which is leaked, depends on the wavelength. Historically, PON systems use the 1310 nm range for the upstream and the 1500 nm range for upstream transmission. In the following Figure 7, the wavelength allocation for different PON systems is shown. The established GPON uses the 1300 nm range for upstream (US) and the 1500 nm range for downstream (DS). The most recent variant, the NG-PON2, uses 1520 nm for US and 1600 nm for DS transmission.

![Figure 7: Wavelength allocation plan for different PON systems from APON (1998) to NG-PON2 (2014)](image)

For the bending loss $L$ (dB/m) per metre, the following empirical equation (1) can be given [39]. The bending diameter $D$ is given in mm, the wavelength $\lambda$ in µm, and the parameter $m$ is the so-called macro-bending number.
given by the ratio of mode-field diameter and the cut-off wavelength for the fibre. In the case of a standard single mode fibre, this parameter \( m \) is \( \sim 8.5 \).

\[
L = \exp \left\{ 8.5 - 519 \cdot D \cdot \left( \frac{1}{\lambda_0} \right)^3 \right\} \text{dB/m}
\]

Using the equation (1) the bending loss per metre, or the maximum amount of light, which can be coupled out, can be calculated for different wavelengths, bending diameters. Multiplied with the interaction length the total loss of the tap can be calculated. To avoid permanent damage to the fibre the bend diameter should not exceed the limits given by the manufacturer of the fibre, a typical value is 20 mm, otherwise the risk of damaging the fibre permanently is very high. The interaction length should be short in order to couple the leaked light into a fibre. Therefore, it is assumed this length cannot exceed 10 mm.

\[ L = \exp \left\{ 8.5 - 519 \cdot D \cdot \left( \frac{1}{\lambda_0} \right)^3 \right\} \text{dB/m} \tag{1} \]

The results in Figure 8 show the coupler properties’ dependence on the wavelength. Considering the parameters discussed already, the tap coupler could work quite well in the range of 1500 nm, which is used in downstream direction. The model predicts a loss in forward direction of 0.1 dB and a coupler ratio of -16 dB. On the other hand the upstream direction gives a different view. At 1300 nm the coupler ratio is predicted to be -32 dB, which makes it impossible for Eve to receive the signal.

If we decrease the bending diameter from 20 mm to 12 mm in order to tap more signal power at 1300 nm – but also risking damage to the fibre, the tap coupler has the properties as shown in Figure 9.
In this case a loss in the forward direction of 0.22 dB and a coupler ratio of ~15dB is now estimated for the 1300 nm wavelength range. However, at 1500 nm the loss now increases to 1.2 dB and a coupling ratio of ~6dB is predicted. This large additional loss would raise alarms in the connected devices and the PON might even become non-operational.

These investigations show that a potential attacker has to overcome the inherent physical layer properties of the fibre in order to tap a PON system. If the typical wavelength split of 1300/1500 nm for upstream and downstream respectively is used, only the downstream direction might be attacked/tapped. If the attacker tries to tap the upstream as well, this will be detected by an increase of the fibre system loss by 1.2 dB via the PON monitoring system.

For the most recent PON standards, i.e. NG-PON2, upstream and downstream are at 1530 nm and 1600 nm and only separated by 70 nm (see Figure 7). In this case, the properties of a tap coupler optimized for that wavelength range are shown in Figure 10.

Figure 9: Tap coupler properties in dependence of wavelength (optimized for 1300 nm)
For the downstream direction at ~1600 nm a coupler ratio -13.5 dB and a loss in the forward direction of 0.2 dB is observed. For the upstream direction at ~1530 nm a coupler ratio of about -17 dB and a loss in the forward direction of 0.08 dB is observed. Both values are high enough on one hand to acquire significant optical power for an optical receiver located at Eve, and on the other hand are low enough in order not to be noticed by the PON monitoring system. In this case this represents another method exploiting a security gap between the legitimate receiver Bob and an attacker Eve, and this is addressed in the next section.

3.3.3. Physical Layer Security considering Bob’s SNR advantage

We again consider the same tapping scenario as previously depicted in Figure 4. The basic assumption now is that Eve’s receiver sees a worse SNR as compared to the legitimate receiver at Bob. If a sophisticated code is assumed, that cannot be reconstructed if the SNR falls below a certain threshold, it would be impossible for Eve to reconstruct the message, while Bob can still decode the original data. This principle has been discussed previously in [38] and is shown in Figure 11.
Figure 11: SNR advantage model (source: SENDATE project)

The black curve denotes the uncoded case, while the red curve denotes the coded case. In contrast to a FEC the red curve does not approach the uncoded curve, but rather the value of 0.5. In order to achieve such a coding behaviour, punctured low-density parity check (LDPC) codes have been proposed [39].

To investigate, whether or if at all this SNR advantage is able to be exploited by Eve, the following assumptions have been made. The PON network consists of a feeder fibre of 10 km length, a 1:64 splitter and a 10 km distribution fibre. Further, it is assumed that the 1:64 splitter has 2-dB excess loss. In addition, the connections and splices at the Tx and Rx account for another 2-dB loss each. Table 3-2 compiles the assumed loss of different network elements.

<table>
<thead>
<tr>
<th>Elements</th>
<th>Loss (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx connector loss</td>
<td>2</td>
</tr>
<tr>
<td>Feeder fibre 10km</td>
<td>3</td>
</tr>
<tr>
<td>1:64 splitter</td>
<td>18</td>
</tr>
<tr>
<td>Excess loss</td>
<td>2</td>
</tr>
<tr>
<td>Distribution fibre 10 km</td>
<td>3</td>
</tr>
<tr>
<td>Rx connector loss</td>
<td>2</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>30</strong></td>
</tr>
</tbody>
</table>

Table 3-2: Loss elements in PON model

If the loss is summed up, a total budget of 30 dB is calculated, which is similar to class C optical distribution network (ODN) as defined in the PON standards. We assume that Eve uses a 15 dB coupler in order to acquire enough optical power and also to remain undiscovered by a potential PON monitoring system. Further, we assume that the upstream and downstream channels are in the 1500 nm range.
We assume that Eve has total budget of 30 dB in order receive meaningful data. Applying all the parameters to the PON network, we can see that Eve can receive a valid downstream signal if a tap coupler is placed anywhere along the feeder fibre (red section). But, any location after the remote node (in the distribution branch), as shown in Figure 12, would exceed the available budget. So, the original data cannot be reconstructed by Eve (green section). For the upstream connection, it is clear that Eve can tap the network at any point in the distribution section of the network and would be able to reconstruct the original message (Figure 13). Since each ONU is connected via a different branch to the remote node, Eve would be forced to install couplers to all branches, which is a significant disadvantage.

![Figure 12: Vulnerable sections in PON downstream](image1)

So, in theory Eve can still capture all traffic assuming 15-dB tap couplers and the same wavelength range for up- and downstream, when using the ‘SNR advantage’ principle.

In order to make it impossible for Eve to acquire meaningful data by placing a tap coupler in the network, the PON operator can install more sensitive monitoring equipment and use a monitoring carrier at a longer wavelength, e.g. at 1680 nm. If we assume the operator can detect loss events of 0.05dB or more at a wavelength of 1680 nm, the following coupler characteristics can be derived.

![Figure 14: Tap coupler properties in dependence of wavelength (optimized for 1680 nm)](image2)
In this case Eve can only use a 30 dB coupler in order to be below the detection threshold of the PON monitoring system. As this would already consume the entire loss budget Eve cannot acquire enough optical power in order to reconstruct the original data sent in the downstream or upstream directions.
4. Conclusions

In this deliverable D2.6 we have discussed the role of impairments when considering physical layer security in 5G networking, both from a wireless and wired perspective. We have performed a fundamental analysis on how physical layer principles can be exploited in 5G wireless networking to generate symmetric random keys between transmitting and receiving nodes, based upon the shared randomness of multi-path channels between the communicating parties. We have considered the effects of noise, path-loss, shadowing, multi-path interference and fading in the wireless segment of the network, using RF/mmW frequencies, or at optical frequencies, e.g. for visible light communications (VLC) using either LED- or laser-based transmitters. We have discussed how the channel reciprocity and entropy in such random wireless channels can be exploited to create symmetric keys, with the channel state information (CSI) being exploited via uncorrelated channel phase, received signal strength, and quantisation, combined with privacy amplification (i.e. to maximise available entropy) to generate sufficiently strong keys.

We have also described the physical layer implications for security in wired (fibre optic) links, when tapping couplers are employed by an eavesdropper in order to evanescently intercept optical communications between transmitting (Alice) and receiving (Bob) nodes. In particular, the issues of such eavesdropping in a 100G OFDM-PON context are described, and how the different power levels and wavelength allocations in other PON architectures such as GPON, NG-PON2 can have an influence on the ability for “Eve” to successfully eavesdrop without the PON monitoring system noticing. Finally, the danger of the SNR advantage model, where a “security gap” can potentially occur in such PON systems is described, along with the punctured LDPC code that can be employed to mitigate against such an attack.

The theoretical PLS techniques described in this report can find application in the wireless and wired segments of future 5G networking, and complement the higher-layer end-to-end security approaches (e.g. e2e virtualised security) that have already been implemented and described in the CHARISMA project.
References


# Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASBG</td>
<td>Adaptive Secret Bit Generation</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>C-RAN</td>
<td>Cloud Radio Access Network</td>
</tr>
<tr>
<td>CSI</td>
<td>Channel State Information</td>
</tr>
<tr>
<td>D-H</td>
<td>Diffie-Hellman</td>
</tr>
<tr>
<td>DMT</td>
<td>Discrete Multi-Tone</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DS</td>
<td>Downstream</td>
</tr>
<tr>
<td>EM</td>
<td>Electro-Magnetic</td>
</tr>
<tr>
<td>GPON</td>
<td>Gigabit Passive Optical Network</td>
</tr>
<tr>
<td>LDPC</td>
<td>Low-Density Parity Check</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>LoS</td>
<td>Line of Sight</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input Multiple Output</td>
</tr>
<tr>
<td>NG-PON2</td>
<td>Next-Generation Passive Optical Network 2  [40 Gb/s capacity]</td>
</tr>
<tr>
<td>ODN</td>
<td>Optical Distribution Network</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>OLT</td>
<td>Optical Line Termination</td>
</tr>
<tr>
<td>ONU</td>
<td>Optical Network Unit</td>
</tr>
<tr>
<td>OTDR</td>
<td>Optical Time Domain Reflectometer</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PLS</td>
<td>Physical Layer Security</td>
</tr>
<tr>
<td>PON</td>
<td>Passive Optical Networking</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RSS</td>
<td>Received Signal Strength</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received Signal Strength Indicator</td>
</tr>
<tr>
<td>SMF</td>
<td>Single Mode Fibre</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal-to-Noise Ratio</td>
</tr>
<tr>
<td>SSMF</td>
<td>Standard Single Mode Fibre</td>
</tr>
<tr>
<td>US</td>
<td>Upstream</td>
</tr>
</tbody>
</table>

(END OF DOCUMENT)