Physical Layer Security in the Last Mile Technology of Mobile Networks

Özge Cepheli[1], Volker Lücken[2], Güneş Karabulut Kurt[1], Guido Dartmann[2], Gerd Ascheid[2]

I. Abstract

Mobile networks have become very widely used in recent years, with expanding possibilities for usage ranging from personal life to business needs. This increased usage has brought more security problems and the importance of maintaining security has been also raised. Mobile networks consist of two main parts, including wired backhaul and wireless last mile. Wired backhaul is the part between base station and the core network. It is a highly reliable network with high data rates. Security in this part is very important. In its cable-based physical layer — the part where physical signals are carried — data is hard to acquire, as physical protection of cables and devices is possible. The last mile is the last part where the user is served. This link has to be wireless for the mobility of users. Wireless medium has an open nature, hence wireless links are more vulnerable to physical layer attacks compared to their wired counterparts. In this chapter, a general understanding will be given on why wireless technologies are often chosen as a last mile technology and why maintaining security is a challenge; moreover the current and future solutions to protect the wireless last mile from physical layer attacks will be explained.

II. Introduction

Mobility has become a very important part of today's communication networks. Over the years, users have changed their preferred platform to access hldata by using mobile technologies instead of conventional desktop devices. From user statistics, it is easy to see that the share of mobile and tablet users are in an increasing trend for website access [1]. As an example, Fig. 1 shows the percentage of users that accessed the websites which use StatCounter [1] using desktop, mobile and tablet devices. Here, we can easily see that users prefer to use mobile platforms lately, and the trend shows that the increase of usage is likely to continue in the near future. As wireless technologies are evolving, users demand higher data rates, increased reliability and security for their mobile connections. However, maintaining those requirements are not easy, as mobile networks are especially vulnerable to failures, intrusion, and eavesdropping. Also the possibility of movement of users, subnets and even base stations increases the challenge. The wireless medium, which is used to carry the signals to the mobile user is usually less reliable, rapidly changing and open to eavesdropping attacks. In addition to all these challenges, the mobile network should survive intentional and unintentional (natural) threats.

The selection of the wireless communication channel for future network deployments is almost certain despite its insecure nature, when compared to the wired counterparts. The wireless channel, however, introduces new threat types that are not addressed with classical security solutions that mainly target the security of the wired

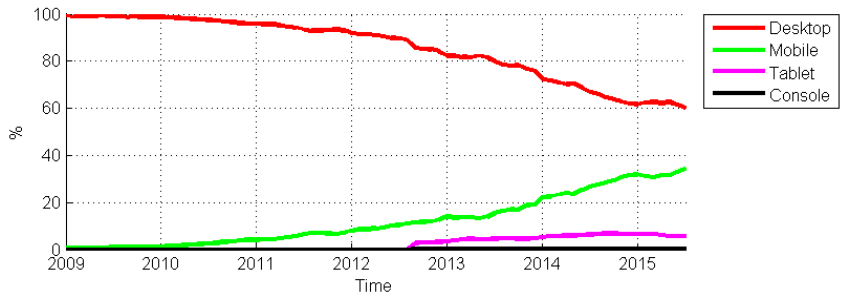

Fig. 1. Worldwide platform usage statistics acquired from StatCounter Global Stats between December 2008 and June 2015 [1]. The share of mobile and tablet users are in an increasing trend.

backhaul links. To address the security threats due to the wireless channel, physical layer security measures that are custom-designed according to the channel status are utilized.

Considering wireless communication networks, there are many natural challenges such as channel impairments and limited transmission bandwidth. Moreover, there can be adversaries which try to perform various attacks to capture or prevent the communication between legitimate parties. Physical layer security addresses detection and mitigation of these attacks along with considering the wireless channel attributes.

The basic system that can be defined for physical layer security consists of three nodes, one legitimate transmitter, one legitimate receiver and one eavesdropper, which are often referred to as Alice, Bob and Eve, respectively. By making use of this basic system, most of the physical layer techniques can be analyzed. Note that this basic model may represent the wireless last mile of a bigger communication network, for example a mobile network where Alice is the base station and Bob is the mobile user for the downlink. Throughout the chapter, the same approach will be resorted to for addressing the physical layer security issues of mobile networks. We will analyze the last mile technology of the mobile networks as a seperate wireless network, apart from the rest of the whole network which is often wired.

In this chapter security in the wireless last mile technologies will be described in detail. Section III introduces the last mile concept explaining the importance of the last mile technology and the security challenges when wireless technologies are used as the last mile. Section IV explains all the fundamentals of wireless channels and attacks, to give a complete picture. Section V explains the security measures used today and Section VI details the security measures in the literature that are the candidates for being a part of the future installations.

III. Last Mile Technologies

In order to provide a diverse set of services, an end-to-end communication link consists of many components addressing different functions. The scope and quality of these services are derived by the requirements and demands of the *end-user*, the user that needs and will use services. The major entities which provide services to enable an end-user to reach another are network service providers (NSPs) and Internet service providers (ISPs). NSPs construct global networks and lease bandwidth to regional NSPs, which offer the bandwidth to local ISPs. Local

ISPs provide and manage services to end-users. Hence, the overall network is maintained as separate blocks and various technologies can be used in each block. According to this structure, Internet backbone, ISP network and end-user network can be designed and operated almost separately.

There are many different media that are used when a communication system is considered as a whole between sender and receiver. However it is possible to divide the communication process into smaller modules for easier analysis. In commercial mobile networks, the *backhaul* of any network uses a highly reliable bandwidth-rich physical medium for the transmission of the communication signals. This implies making use of a wired infrastructure, such as fiber optic cables.

The standard that is used to establish the final connectivity link between the service providers and the end-user is referred to as the *last mile technology*. Unlike the backhaul, the last mile technology also depends on the requirements of the end-users, where coverage and cost may become more important than reliability and data transmission rate. Wireless technologies are prominent candidates as the last mile technology. They provide a good compromise, as they enable user mobility and ease of use, which are very important on new generation mobile technologies. The usage of mobile devices and mobile communications is rapidly increasing within the technology users [2], [3]. The fact that the wireless technologies can not achieve the reliability and data transmission rate of a wired counterpart becomes a secondary concern.

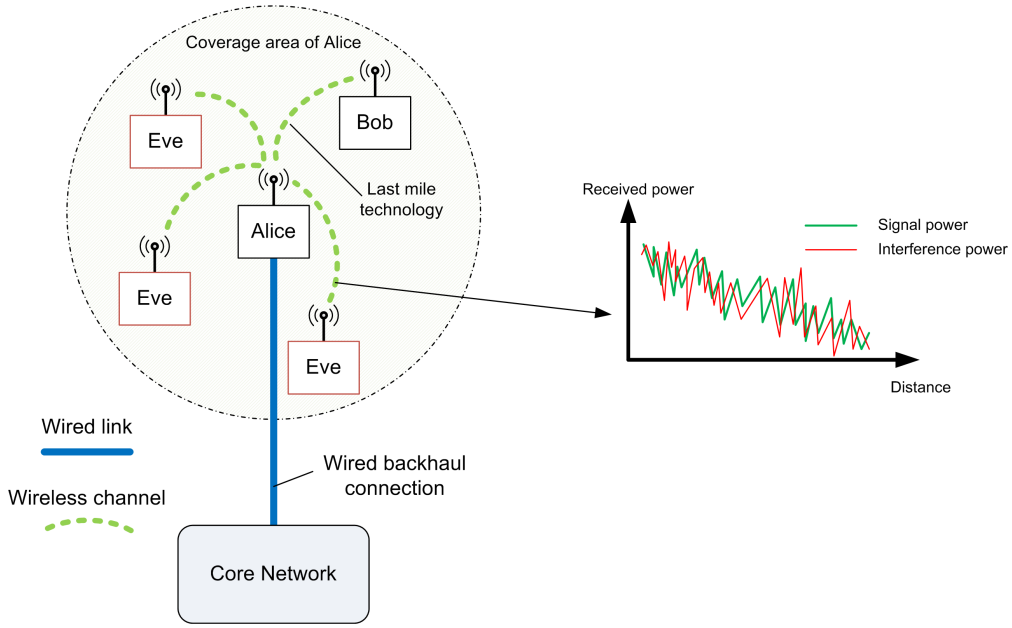

Fig. 2. Wireless communication as a last mile technology. The wireless channel characteristics increase the security threats due to the open nature of the channel. In the figure there is a legitimate wireless transmitter called Alice who is connected to the core network by a wired connection and use the wireless medium for the last mile connection to communicate with the legitimate receiver, Bob. As wireless medium has an open nature, illegitimate receivers are also able to gather the signals from Alice. The power of the received signal on Eve is dependent on the distance and fluctuates due to channel characteristics such as multipath fading and shadowing. Interference from other resources are also received in the same way. Note that interference has a big effect on the signal quality. In this case, why not use as a security countermeasure? We can whisper nonsense signals to Eve's ear to improve secrecy - and it is called artificial interference.

A. Choosing wireless as a last mile technology

Wireless networks have become a major part of communication networks today, and also appear to be a strong component of the future communication networks. Besides 4^{th} generation (4G) and 5^{th} generation (5G) mobile systems, the family of IEEE 802.11 standards are being employed by a large fraction of broadband users to connect their computers to Internet for the last mile. This means that wireless technologies are very likely to be utilized as the last mile technology in the future as well. The main reasons to choose wireless technologies is the mobility and ease of use. In fact, according to Mary Meeker's KPCB 2015 Internet Trends report [4], the percentage of the time spent on mobile digital media in the US is already higher at 51%, when compared to desktop with 42%. The use of wireless technologies comes at a price of bandwidth scarcity and security issues. The disadvantage associated with lower data transmission rate is easily overlooked as newer wireless technologies have higher data rates, however the security issues are critical in wireless technologies due to the open nature of wireless links. Besides the security threats from upper layers of OSI model, using wireless medium brings particular vulnerabilities to the physical layer. Note that besides the apparent use of wireless medium in mobile networks, even for broadband Internet connections the wireless technologies are being considered [5], [6]. Hence, when we mention wireless physical layer security, most of the commercial networks like mobile networks and future broadband networks are addressed.

B. Importance of last mile for security

As already mentioned earlier, the main security challenge of wireless technologies as the last mile is caused by the open nature of the wireless channel. In conventional cable networks, the physical layer medium consists of cables and the signal transmission over a cable between two nodes is considered to be safe. This is an accurate assumption as the security of a cable could be easily achieved by physically making the cable unreachable, for example by using locked server rooms or underground cables. The eavesdropping attack, which is performed by illegitimate users to capture data by listening to the link becomes very hard to be successful when the cables are unreachable. However in wireless communications, instead of using cables to transmit the signals, antennas are used to transmit and receive the signals. The signals experience some changes in power and phase after leaving the transmitter antenna before reaching the receiver antenna. However, when wireless channels are used to transmit signals, the signal can reach anywhere within the transmission range, i.e. where an acceptable signal to interference plus noise ratio (SINR) level is available. Service providers have to keep the SINR above an acceptable level for their users, which is a constraint for successful reception of the signals on the receiver side. However, the SINR level for illegitimate users may also be enough for them for successfully capturing the transmitted data, which leads to a major security issue considering the eavesdropping attack. For signals transmitted from an antenna, there is a spatial pattern that signals are spread, and the signal strength decreases by distance, which will be explained in detail in the next section. For the spatial definition of signal strength's being above some level is termed as the *antenna range*. This defines the locations that the signal can be received successfully. Every user within the transmission range, including the illegitimate receivers such as eavesdroppers, can capture the transmitted signals.

A typical mobile network with a wired backhaul is shown in Fig. 2. In the figure, the wireless transmitter antenna is referred to Alice and is connected to the core network by a wired link. Alice is the legitimate transmitter,

transmitting signals to the legitimate receiver Bob, whereas the signals are also received by illegitimate users, referred to as Eves. The received power of signals from transmitter antenna versus distance is also shown in the figure, which is caused by the inherent properties of wireless channels, like path loss and shadowing. These properties will be thoroughly explained in the next section. In the given setting, it is clear that security of the overall network is affected by the security of the last mile. Although the core network security threats can be addressed by the conventional security solutions, the security of the wireless last mile remains a challenge, that should be addressed with physical layer security measures that are custom-designed according to the wireless channel. Throughout this chapter, the current approaches will be introduced along with classical solutions and main concepts, to analyze this challenge.

IV. Physical layer Security Fundamentals

A. Properties of wireless channels

In a basic wireless communication scenario, electrical signals are converted into electromagnetic waves through an antenna and these electromagnetic waves are broadcast from the transmitter. These waves are then captured by a receiving antenna and signals are obtained at the receiver side. The impact of the physical phenomena that signals experience while traveling from transmitter to receiver is taken into account by using wireless channel models. There are different channel models that are frequently being used in the literature such as Rayleigh, Rician or Nakagami-m fading channel models [7], as well as Stanford University Interim (SUI) [8] or 3GPP WIM2 [9] models. Channel effects as path loss, shadowing, fading (small scale and large scale) and Doppler shift are usually included in these models. Interference, which is the additional electromagnetic signal received along with the intended signal, is another major cause for signal quality degradation and is usually modeled independently.

Looking from a system level, in order to study the eavesdropping case, Wyner [10] introduced the wiretap channel, which is a special channel scheme where the eavesdropper's channel is a degraded version of the channel of the legitimate user. In the study [11], the authors considered a general independent channel condition, by eliminating the degraded eavesdropper channel assumption and studied the transmission. Note that the studies were not considering wireless channels directly, however became fundamental studies in physical layer security in wireless networks as channel definitions not only comply with wireless channel models but also cover eavesdropping in wireless channels perfectly. Since multiantenna technologies are now frequently used, many studies have been conducted with various antenna configurations, as single-input-multiple-output (SIMO) [12], multiple-input-single-output (MISO) [13]–[15] and multiple-input-multiple-output (MIMO) [16]–[19] channels.

1) Thermal noise: Both wired and wireless communication systems are subject to random fluctuations on the signal received levels, which are caused by many natural sources. Referred to as *thermal noise* or *additive white Gaussian noise*, this phenomenon is generally modeled with a Gaussian (normal) distribution.

2) Path loss and fading: Path loss refers to the weakening of the signals as they propagate through space. This weakening is caused by the distance between transmitter and receiver. In addition to the path loss, the magnitude and phase of the received signals over the wireless channel may rapidly change in time, frequency and space [20]. Referred to as *fading*, this effect is usually modeled as a random process. There are two main classes of fading,

namely the *large-scale fading* and the *small-scale fading*. Large-scale fading is caused by path loss and shadowing by large objects (such as buildings and hills). The large scale fading is typically frequency independent and frequently modeled by log-normal shadowing. Small scale fading is generally caused by the interference generated by the existence of multiple transmission paths between the transmitter and receiver, and it is frequency dependent. Most frequently used small scale fading models are Rayleigh, Rician, Weibull, Nakagami fading models.

It is also very useful and widely used to classify fading according to the rapidness of the changing compared to the signal. When the channel conditions change faster than the symbol duration, it is called as *fast fading*, and similarly it is called as *slow fading* when the channel conditions change slower than the symbol period. Fast fading can occur due to the relative motion between the transmitter and receiver objects, which is known as Doppler spreading.

3) Multi-user interference: When modeling the wireless channel effects, it is essential to consider *multi-user interference*, which is the signals of users or technologies that are captured by receiver. Basically, the receiver antenna captures not only the signals of the intended transmitter, but also a superposition of signals of all the transmitters using the same frequency band that have the receiver in their antenna range. These signals, also subject to fading and path loss, act as an impairment. They are often very strong, severely limiting the SINR values, possibly causing communication disruptions. Additionally, other than natural ambient interference sources, interference can be generated deliberately by an adversary. In this case, this approach is referred to as a jamming attack.

The impact of wireless channel is very important when security is considered, as the performance of physical layer attacks are usually based on accurate channel estimation for both attacker and legitimate user channels.

B. Attacks

In wireless communication networks, the adversaries attack one or more of the four main system security requirements which are secrecy, authentication, data integrity or robustness. *Secrecy* defines the discreteness of the data between the origin and destination. *Authentication* is the act of confirming that the destination of the data has the access rights. *Data integrity* refers to the completeness and originality of the data during its life cycle. Lastly, *robustness* is defined for the communication system to remain operational under degrading effects. Major attack types are listed in Fig. 3 along with their target requirements. This table can act as a basic reference for attacks rather than being a complete list of all attacks. It is a very hard task to cover attacks, as new attack types are being discovered everyday. Following the latest discovered attacks is a crucial requirement for having up-to-date information on current security vulnerabilities of any system.

Physical layer targeted attacks can be classified into two groups; passive or active attacks. In *passive attacks* the adversary does not give provide input to the system, making these types of attacks is very difficult to detect. On the other hand, during *active attacks* the adversary uses a transmitter, actively interfering to the network. These attacks are usually easier to detect, however this does not imply that they are easy to prevent. Physical layer targeted attacks can also be grouped by their targeted security requirements; namely the secrecy, authentication, data integrity and robustness.

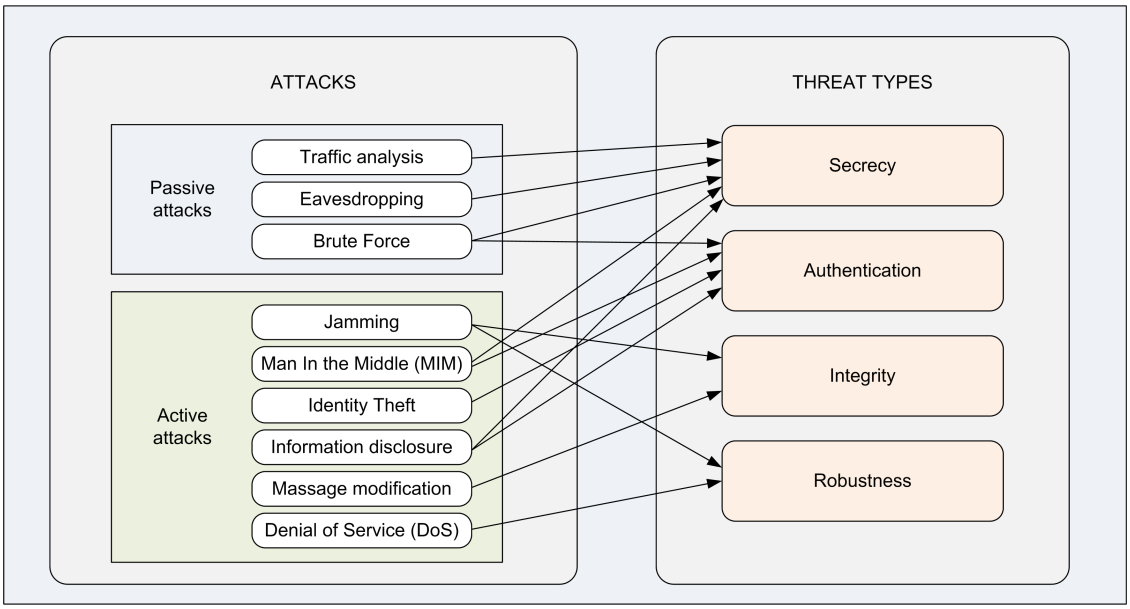

Fig. 3. Physical layer attack types and targeted system security requirements. Attacks are classified according to the activity level of the adversary and the threat types.

1) Secrecy attacks: Major attack types against data secrecy are eavesdropping and traffic analysis attacks. *Eavesdropping* is the act of secretly listening to the private conversation of others without their consent, which projects to gathering of wireless communication data by non-legitimate users. Eavesdropping attacks are typically very easy to perform and very challenging to detect due to their passive nature. Such attacks can be executed by properly tuned reception and decryption of the encrypted data, in case data is encrypted. The eavesdropping attack can be implemented in either real-time or non-real-time fashion. The non-real-time eavesdropping is more critical as the adversary can use brute-force based approaches with high computational complexity to capture the data that may take a longer time to compute.

Also a passive attack, *traffic analysis* is a similar version of eavesdropping attack, where the non-legitimate user cannot intercept the communication data but gathers the traffic information, like transmitter/receiver identities or data rates. Usually traffic analysis attack is performed where the secret key used for encryption cannot be obtained.

Main classical countermeasure to eavesdropping attacks is encryption. There is no particular classical security measure for traffic analysis. The recently proposed beamforming and artificial noise based physical layer security approaches can aid combat with passive secrecy attacks, including traffic analysis attacks [21]–[25].

2) Authentication attacks: Authentication is the process of confirming legitimacy of a transmitter. Most frequently encountered authentication attack types are brute-force, eavesdropping, man in the middle (MIM) and identity theft attacks. These attacks are also detectable in physical layer.

In *MIM attacks*, the adversary makes independent connections with the target nodes (performing two-way communication) and transmits messages among them, impersonating each destination making them believe that they are communicating with directly to each other. MIM attacks also include eavesdropping attacks. In fact, during

a MIM attack, the entire conversation is controlled by the attacker. Beyond the secrecy violation, it is clear that MIM attacks can be very dangerous to systems as the attacker gets authenticated and it is able to enter the system or change the communication data in a harmful manner. In an *authentication cloning attack*, an unauthorized user pretends to be a legitimate user by deceiving the authentication system. An authentication cloning attack can be implemented in many ways, including capturing the authentication sequences that are based on physical layer attributes. For example, an intruder can imitate its location or channel information as the legitimate user and get authenticated to access resources.

Identity (ID) theft attacks are usually performed by capturing and detecting network traffic data and identifying node with network privileges. Most wireless systems allow some kind of ID filtering to allow only authorized device with specific IDs to gain access and utilize the network. Identity information can also be gathered by executing brute force attack, which means trying all the possible ID key options.

3) Data integrity attacks: Data integrity attacks compromise from the trustworthiness of transmitted data over the communication life cycle. Frequently observed data integrity attacks are message modification and jamming attacks. Attackers can transmit fake control, management or data frames over wireless channel to mislead the receiver. *Message modification* is the general class of attack types that based on additions or deletions to actual data by adversaries. *Jamming* attacks are based on transmitting signals to disrupt communication link, by limiting the SINR. Jamming attacks can result in partial disruptions as well. Authentication based attacks can also lead to data integrity problems, as altering data is a possible after the authentication of the adversary.

In order to detect data integrity attacks, integrity checks, such as key-based techniques or pre-determined packet headers, can be performed. Note that although such attacks may not always be detected, integrity checks are still an efficient way to deal with physical layer related errors during transmission. Such errors can also be combatted using error control coding or automatic repeat request techniques.

4) Robustness attacks: Robustness in wireless networks mainly implies the strength of the communication system against channel impairments. The major robustness attacks are denial of service (DoS) attacks. A *DoS attack* targets exhaustion of network resources to disrupt communication among legitimate users. Jamming is the most frequently observed DoS attack type at PHY. DoS attacks may also be executed by a number of distributed adversaries to reduce their detection probability, and are named as *distributed DoS (DDoS)* attacks and considered as one of the most challenging security issues in current communication systems. DDoS are attacks are considered as of the most challenging security issues in current communication systems.

Countermeasures of DoS or DDoS attacks are not clear as these attacks can be executed in various ways. Anomaly detection systems are used to determine if an attack is being held for any of the network resources. In order to prevent a detected DoS attack, the resource usage of the adversaries is blocked or a back-up resource is used. If a DoS attack is detected, the network controller node usually prevents the adversaries by blocking their resource usage. Another approach to enhance the robustness of a system is to diversify network resources by using back-up resources. These back-up resources can be used if one resource is under attack. For example, if a jammer is detected, the wireless network may switch to a different carrier frequency to avoid the quality degrading effects.

Usually systems are designed to have back-up communication lines in different networks to avoid connection

losses. Robustness can also be achieved in the device side, wireless systems can be designed to have back-up devices that can be switched to, if the master device is under a physical attack.

C. Performance metrics of physical layer security

The fundamental issues of secure channel capacity have drawn much attention in the information theory community in recent years. Most of these works focused on *secrecy capacity*, which refers to the maximum rate of secret information sent from a wireless node to its destination in the presence of eavesdroppers. This metric is very useful as it stands as an information theoretical measure of the security of a channel. Using such a metric, it is possible to compare channels and to measure how much security is gained using a security countermeasure. It is shown by Wyner [10] that the perfect secrecy capacity is the difference of the capacities for the two users in discrete memoryless channels. This result has been generalized to Gaussian channels by Leung et al. [26] then by [27], considering the full channel state information (CSI) case. The secrecy capacity under full-CSI assumption is adopted as an upper bound for the secrecy capacity when only the CSI of the legitimate receiver is known at the transmitter. The authors in [27] also proposed a low-complexity on/off power allocation strategy that achieves near optimal performance with only the main channel CSI. This scheme was shown to be asymptotically optimal as the average signal-to-noise ratio (SNR) goes to infinity. The authors in [28] extended the previous studies considering imperfect CSI case. Based on an information-theoretic formulation of the problem, in which two legitimate partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through a second independent quasi-static fading channel, the role of fading is also characterized. In [28], the authors define the secrecy capacity in terms of outage probability and provide a complete characterization of the maximum transmission rate at which the eavesdropper is unable to decode any information. The results of this study is generalized into multiple eavesdropper case in [29] and the secrecy capacity of the system is analyzed in terms of outage probability and outage capacity. In [12], the authors define the ergodic secrecy capacity and find the optimal power allocation at the transmitter that achieves the secrecy capacity for the full-CSI and no-CSI cases along with the analytical expression for the lower bound of ergodic secrecy capacity is presented. They also give the analytical expression for secure outage probability to study the secure outage performance of their proposed model. Below we classify main metrics for physical layer security performance.

1) Information theoretical metrics: Information theoretical metrics are widely used in the literature, for the mathematical assessment of security. The upper bound of perfectly secret transmission rate from the legitimate transmitter node to a legitimate destination node is defined by the secrecy capacity [10]. The *probability of outage in secrecy capacity (OSC)* is another important concept in the information theoretical analysis of physical layer security approaches. OSC is defined as the probability that the instantaneous secrecy capacity being less than a target secrecy rate.

2) QoS related metrics: Clearly, SINR value of the channel is directly effecting both the secrecy capacity and the OSC. However, SINR also dictates the performance of a communication link, hence is considered a quality of service (QoS) related performance metric [21]. A sufficiently high (low) SINR value enables robust transmission with a maximum (minimum) desired error level. Hence, when considering a transmission from Alice, lower bounding the

SINR of Bob and upper bounding the SINR of Eve can lead to reliable and secure communication. The SINR can be changed by using the physical layer security techniques, such as beamforming approaches, as will be described in Section VI. Note that the SINR is reduced to SNR in the absence of multi-user interference.

The received signals are demodulated and decoded to bits at both Bob and Eve. At the output of the decoder, it is possible to calculate (or estimate) the *bit error rate (BER)*, which is one of the primary performance measures for robustness of digital communication systems. BER is always related to SINR, however modulation and coding techniques have different BER performance on the same SINR level. Usually a minimum BER requirement is defined for a successful communication, depending on the desired application. If BER of a system is below a minimum required level, a communication link cannot be properly established. As a result, it can be seen that forcing a unsatisfactory BER on unauthorized nodes can actually improve the network security. Hence, BER can also be used to define the QoS and the physical layer security level of a system. When considering BER as a performance metric, the impacts of the selected modulation and coding schemes are also taken into account. Also note as a function of BER, the frame or packet error rates can be considered as performance metrics of physical layer security.

V. Current Physical Layer Security Solutions

Security is hard to maintain on operational networks with large volumes of data, analysis and detection of security threats become very challenging when delay and data rates are important. There are several classical tools to protect networks against attackers. Ideally, all tools work collectively, minimizing maintenance requirements while improving the security level [30]. The most common way to protect a network is to make use of tools such as anti-virus and anti-spyware software, firewalls, intrusion detection systems (IDSs), intrusion prevention systems (IPSs) and virtual private networks (VPNs) for upper layers along with encryption and spread spectrum based eavesdropping mitigation techniques in the lower layers.

A. Network security solutions

Generally, network security solutions target the network layer of OSI reference model. At its most basic, an *IDS* provides passive protection by observation of data network from a monitoring port (such as a tapped communications port); comparing the observed data traffic patterns with the pre-defined rules and patterns. This may not always be an effective solution for today's fast evolving networks due to possibly rapidly changing attack traffic patterns.

Jammer detectors are a good example of physical layer IDS, where special devices are used to detect the existence and the source of a jamming attack [31]. There are many commercial off-the-shelf jammer detectors available today.

IPSs simply add more security throughout the network by not solely monitoring and alerting but also stopping the traffic flow which may be malicious or harmful in a proactive approach. Also note that, the probability of false positive decisions when using the IPS approach for data networks may erroneously cause communication disruption.

In addition to IDS and IPS tools, recently, web application firewalls (WAFs) are started to be deployed for defending against attacks. Currently, WAFs are very effective at certain attack types where IPSs may not successfully

prevent (such as HTTP request based attacks). WAFs lack providing security in lower layers whilst their focus is in only on application layer.

B. Encryption solutions

In encryption based security solutions, data are encrypted using a *secret key*, enabling only authorized recipient to decrypt. The algorithm that carries out the encryption is called *cipher* and the ciphers depend on some auxiliary information, called a secret key. Secret key is usually a randomized code-word, shared between the transmitter and the recipient and used to encode the original data called as plaintext into ciphertext. Decryption step can be successful if the transmitter and the receiver have the same key pair, and any person who seizes the key can solve all encrypted communication.

Encryption is possible in all layers of OSI model, and the approach usually named according to the target layer. Application layer (layer 7), network layer (layer 3) and data-link layer (layer 2) encryption techniques are the most common methods that are used in today's networks.

Encryption is the key concept for *virtual private networks (VPNs)*, which is the extension of a private network across a public network. VPN is used to establish a secure connection between two sites, where the sites connect through a public network. The traffic is secured by using encryption and tunneling protocols so that the connection stays private from the other users in the public network.

In lower layers, security is mostly maintained by encryption solutions in data link layer. Encrypted data should be decrypted before its content can be revealed by an attacker. In order to decrypt the data, one should have the secret key in hand, which is ensured that only possessed by the legitimate receiver [32]. However, the key can be acquired by a brute-force attack or *exhaustive key search*, which is simply trying every possible key combination until obtaining the correct key. Note that every encryption key can be discovered, but within a significant time range that is dependent on the processing power and the length of the key. Hence, if data should be secure for a long time, a long key should be used for encryption, which causes more power consumption for the encryption and decryption processes, and affects the battery life of mobile devices.

The selection of encryption technique is a sensitive subject. Usually the best option is to use a strong well-known encryption standard, which is already tested for many years against a diverse set of attack types. Novel encryption algorithms comes with the risk of having security holes which may enable attackers to easily retrieve the secret key. Moreover, longer keys should be selected for increased security.

C. Spread spectrum based eavesdropping mitigation techniques

For many years, secure wireless communication systems are being developed, many with a military context as background. One of the earliest proposals of spread spectrum techniques was the frequency hopping patent from Antheil and Lamarr in 1941 [33], which describes a simple frequency hopping system for the wireless control of torpedoes. Based on a predefined synchronized sequence of carrier frequencies, which are stored on paper punch cards, the system was intended to provide secrecy and jamming robustness. Later, more sophisticated spread-spectrum techniques like *code division multiple access* (CDMA) have been developed for a use in both military

and also personal wireless communications. For the civil wireless communications, the security aspect was mostly a minor factor in the design of spread spectrum waveforms and practically, security was not fully realized. Still, the waveforms used have the capability to significantly increase the security (secrecy and jamming-robustness) performance of a communication link in principal. Especially with the more recent focus on secure and private personal communications in mind, these waveforms can prove suitable.

The definition of spread spectrum techniques is that the transmitted signal uses a bandwidth that is independent of and significantly larger than the information bit rate, and further, demodulation can be performed by correlation of the receive signal with the spreading signal [34], [35]. In the field of spread spectrum techniques, different types of waveforms and realizations exist. The most important ones are the *frequency hopping spread spectrum* (FHSS) and *direct sequence spread spectrum* (DSSS) types. FHSS, which already was employed in the initially presented system from 1941, is realized using a time-dependent carrier frequency of the transmit signal. Each frequency position is held for a specific time, the so-called *dwell time* [36]. DSSS, in contrary, uses a modulation of the information signal with a spread sequence, which usually has a higher data rate than the information signal itself, and therefore leads to a frequency spreading.

The widely-used frequency hopping offers a protection against casual eavesdropping and jamming attacks, but does not offer a significant secrecy increase in practice, as especially in a situation with only a single hopping signal in the channel, it can be easily tracked and the hopping sequence can be recovered afterwards. In the final communication system, the hopping sequence is pre-shared or exchanged between the legitimate users in prior. Even with the practical disadvantages mentioned, a real system with a hopping rate can especially hinder jamming attacks, where the hopping steps cannot be predicted in a live scenario. Further, the impact of narrow-band interference can be reduced.

DSSS techniques are very relevant in current mobile communication standards. In the *Universal Mobile Telecommunications System* (UMTS) 3G standard, *Wideband CDMA* (W-CDMA) is used which is a very high bandwidth version of CDMA. From the secrecy point of view, however, there are some reservations because of implementation issues of the spreading sequence in the standard [37]–[39]. Also, CDMA is used in many security-critical military applications, as it both strongly reduces the risk of interception by eavesdropping and the risk of jamming. CDMA is realized by multiplying the input data with a pseudorandom noise (PN) sequence. Multiple access is then implemented by using orthogonal sequences (spreading codes) for each of the users. This offers an inherent separation, even with all users occupying the same frequency band and transmitting at the same time. Using specific long and more complex code sequences, high secrecy levels can be reached [37]–[39].

One main disadvantage is that for the current plannings for the 5G, CDMA techniques only play a minor role. This is why some alternative techniques, for example for the prospective 5G waveform *filter bank multicarrier* (FBMC), are under development and described later in this chapter.

VI. Future Physical Layer Security Solutions

As physical layer security is an emerging topic, there are many new techniques and approaches that have been proposed which not yet implemented in the current security solutions. We group these approaches into three major

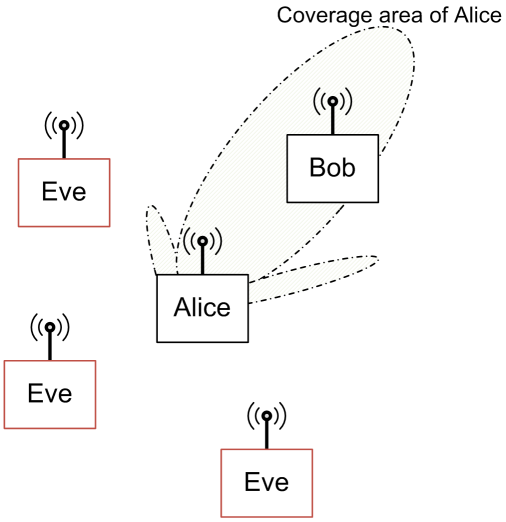

Fig. 4. Adaptive beamforming can be done by Alice having multi-antenna transmitter by calculating the necessary phase components of each antenna component to create the antenna pattern focused on Bob.

titles as signaling based solutions [21]–[23], [40]–[44], filter based solutions [45], [46] and physical layer key generation techniques [47]–[52]. The considerations on implementation of these new techniques in future mobile networks will also be discussed at the end of the section.

A. Signaling based solutions

1) Beamforming: Beamforming is a multi-antenna technique that enables the transmitter to spatially focus signals by adaptively adjusting the amplitude and/or phase of each array element. With transmit beamforming, one can utilize the spatial shaping to degrade the reception performance of eavesdroppers [40]. Beamforming recently became a viable countermeasure for wireless physical layer security as reception of signals by eavesdroppers can be physically limited [21]–[23].

Early implementations of beamforming are based on *switched beam* techniques that relied on the selection of a of pre-determined beam patterns according to channel characteristics. A more dynamic way to spatially form transmission patterns is to use *adaptive beamforming* systems, where the beamforming coefficients are adaptively calculated in order to reach a specific beam pattern. As a result of beamforming, transmitters can physically focus the signals only on the legitimate receiver hence increasing the secrecy capacity and SINR at Bob, as shown in Fig. 4.

In order to successfully deploy beamforming based security solutions, the channel state information (CSI) of the legitimate receiver should be available at the transmitter. If ideal CSI of the eavesdroppers are also present at the transmitter, then it becomes possible to calculate the optimum beamforming coefficients to maximize secrecy capacity [23]. However, channel information may not be perfectly known, the information can be partial as in [14], [53], delayed as in [13] or imperfect as in [15], [16], [54]. Even if Alice does not possess any information about

TABLE I

ASSUMPTIONS ABOUT EAVESDROPPER LOCATIONS

ine CSI perfectly known	[10], [26], [27], [40], [41], [57]
ine CSI partially known	[14], [53]
ine Delayed CSI	[13]
ine Imperfect CSI	[15], [16], [54]
ine Direction known	[17]
ine CSI unknown	[55], [56]
ine	

Eve's channel, beamforming can be used to focus the signals on the legitimate receiver, which increases the overall security [21], [55], [56].

2) Artificial Noise: Artificial noise (AN), or *artificial interference (AI)* is another countermeasure that is commonly used as a physical layer security solution, in a complementary fashion to beamforming. AN approaches mainly imply transmission of deliberately generated noise signals, in addition to information bearing signals.AN can be generated as legitimate transmitter based as in [41], [42] or legitimate receiver based as in [57]. A new approach is to use friendly jammers instead of legitimate users, as in [18] and [58]. Using AN can be also be interpreted as a jamming attack towards Eve. Clearly, effective use of AN requires beamforming, otherwise AN would effect all the users including the legitimate receiver, Bob.

By using beamforming, it is possible to optimize both information signal and AN to maximize security [23]–[25]. Hence, in order to deploy AN approaches optimally, the CSI of Eve should be available at Alice. In this case, Alice can deploy adaptive AN which targets the eavesdropper only, as shown in Fig. 4. However, if Eve's CSI is not available, AN can still be used in a isotropic manner, which means sending AN everywhere but the legitimate receiver.

Availability of location or channel information of eavesdroppers is an important point of the system model. The practical challenge of gathering information about eavesdroppers result in several approaches to be held in related studies. Major approaches can be summarized (with examples) as in Table I.

Locations of eavesdroppers can be also modeled as a random process as in [59], where the locations of eavesdroppers are modeled by a Poisson point process, and in [60] where the authors study the optimum location of an eavesdropper from a secrecy capacity perspective in multi-terminal networks with power control. Also in [61], the authors consider end-to-end secure communication in a large wireless network, where the locations of eavesdroppers are uncertain.

AN and beamforming techniques are frequently resorted to in theoretical works but their practical considerations is quite recent. This is caused by their high processing requirements and intolerance to CSI estimation errors. However, with increasing processing capabilities of end-user devices we expect to see them in the near-future.

3) Interference shaping based solutions: Interference shaping can be done by making use of beamforming in a multiuser environment, in order to calculate the optimal transmission schema for each user to increase overall performance [43]. Considering the security perspective, it is possible to spatially shape the existing interference to

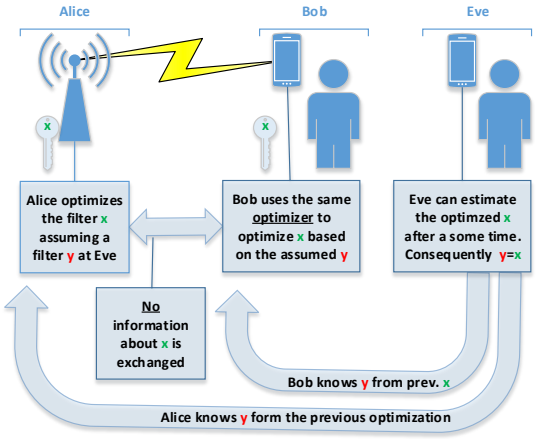

Fig. 5. Idea of optimization aided matched filter design [45].

avoid or reduce AN usage that requires additional transmit power. The natural ambient interference of multicell networks can be tailored not only to maximize the signal to interference and noise ratio (SINR) of legitimate users as in [44], but also to enhance secrecy against eavesdropper attacks, by simultaneously degrading the SINR of the eavesdropper. To achieve such a system, a max-min beamforming problem is proposed in [23] that maximizes both the SINR of legitimate users and the inverse SINR of eavesdropper with a sum power constraint. It is shown that the interference-shaping based techniques accomplish to enhance secrecy in a more efficient way than the conventional AN-based physical layer security systems, often with the cost of higher processing resource requirements .

B. Filter based solutions

More recently, new techniques for waveform-based physical layer security have been investigated, which are still in an initial state, but already provide promising results for the implementation in future wireless communication systems. Two techniques are presented here, which are based on the time-frequency-localization and matching of transmission filters. The first technique presented is an online eavesdropping mitigation technique that is based on the optimization of transmit and receive filters on the sides of the legitimate communication partners in a single-carrier transmission. The second technique is called *filter hopping* (which has no relationship to the similar-sounding *frequency hopping*) and employs the *filter bank multicarrier* (FBMC) waveform, which is a candidate waveform for 5G mobile communications. Based on specific energy-dispersing transmit filters, which are overlapping and varied over the time-frequency-lattice (TFL), the technique allows a strong secrecy capacity increase in a wireless communication system.

1) Single-carrier online eavesdropping mitigation techniques: In [45], an optimization-based matched filter design with improved secrecy is presented. Fig. 5 presents the concept of this approach. The legitimate transmitter and receiver use the same algorithm for the optimization of the matched filter pair. Both, the receiver as well as the transmitter use the same algorithm, therefore, the optimization results on both sides results in the same set

of filter coefficients. The filters are designed such that the signal-to-interference ratio (SIR) is maximized at the legitimate receiver. Furthermore each filter should have a sufficient stop-band attenuation. Secrecy is achieved by a matched filter optimization against an eavesdropper by a reduction of their SIRs. The concept is designed for so-called online-attacks where an eavesdropper tries to get access to an established communication link. After some time, the eavesdropper could potentially estimate the matched filter such that the secret information can be decoded at this illegitimate receiver. Therefore, the legitimate receiver must re-design their matched filter pair after a fixed time period to avoid a reception of the secret information by an eavesdropper in the vicinity. The new designed matched filter is, therefore, designed against the filter estimated by the eavesdropper, which is the filter of the previous optimization cycle.

An advantage of this concept compared to beamforming based approaches is that the optimization does not need any channel state information of the illegitimate link. A weakness of this concept is the potential risk that an eavesdropper can estimate the algorithm itself. This problem can be solved with by random-constraints based on a pre-shared key set similar to encryption keys. Instead of pre-shared keys the legitimate users can also the channel as a random source in case the eavesdropper is sufficiently far away. With these keys, randomization constraints, random filter change period and different initial solutions can be used to design randomized matched filters.

A different approach is a so-called offline optimization. In this case, a large set of randomized matched filters can be shared by the legitimate links. Alice and Bob randomly exchange their matched filter-pair. The selected filter pair must be orthogonal to the previously selected filter pair to ensure a low SIR at the eavesdropper. An open question is: How many of these orthogonal filter can be designed with the given set of secrecy and random constraints. The work [46] is an extension of [45] and based on a offline optimization of large filter set.

2) Multi-carrier techniques: FBMC filter hopping: The second technique presented is the *filter hopping* method [46] for systems using the FBMC waveform. FBMC is a multicarrier waveform like Cyclic Prefix OFDM (CP-OFDM), but it features a per-subcarrier symbol shaping using a prototype filter, which can be efficiently realized by a polyphase filter bank. A major difference is the lattice structure, which is different to the one of OFDM/QAM. For the FBMC case, the lattice structure is called *Offset QAM* (OQAM). This means that instead of complex-valued QAM symbols, twice the rate of real-valued PAM symbols are transmitted. Furthermore, each subcarrier is filtered with the prototype filter, whose frequency response is plotted in Fig. 6. Finally, the Cyclic Prefix (CP) is also omitted, as it is not necessary due to the localization properties of the symbols in the time-frequency-lattice. For comparison, the time-frequency-lattices for both the CP-OFDM and the FBMC waveform are shown in Fig. 7.

Due to the pulse shaping with the prototype filter, which is a major degree of freedom of the FBMC waveform, the symbols are spread in time and frequency domain differently than OFDM symbols, which have a rectangular shape in time domain and a Sinc-shaped response in frequency domain. With a matched receive filter, orthogonality is preserved at the receiver side and no interference is experienced by adjacent symbols in the TFL. The idea of the filter hopping is based on the fact that with a mismatch of the receive filter, the orthogonality conditions are violated and the energy of the transmit symbols is widely spread to adjacent symbols and subcarriers. This effect is even significant with a slight mismatch of the transmit and receive filters. In a practical system, Alice and Bob can exchange the filter design using key exchange techniques or a pre-shared sequence of filters. Then, the filters

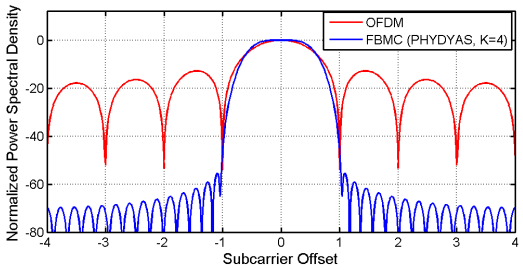

Fig. 6. Spectral comparison of OFDM and FBMC (with PHYDYAS filter).

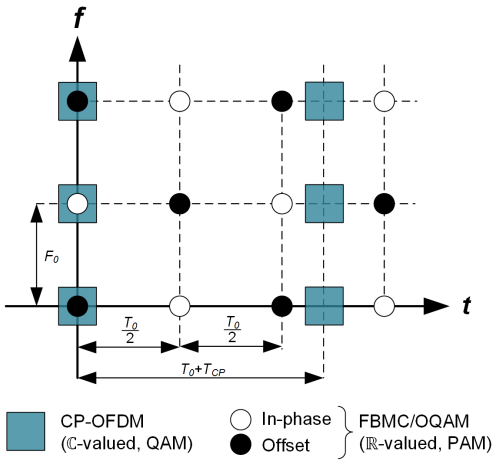

Fig. 7. Time-Frequency-Lattices of CP-OFDM and FBMC/OQAM [62].

are varied over the TFL, either continuously or blockwise. A possible eavesdropper is then required to try a large number of filter sets and designs in order to get an error-free reception.

A proposed transceiver chain design for an FBMC filter hopping system is shown in Fig. 8. It features the time-varying transmit and matched receive filter at Alice's and Bob's side and the eavesdropper, who is using a quasi-static receive filter, as he is not able to follow the sequence of filter changes. The complexity increase due to the variation of the filters in the filter bank is negligible, however, the filter design techniques might inhere a higher amount of processing. Then, Eve will experience interference on its receive signal, leading to a degradation of his SINR in a large number of possible channel conditions. By that, a secrecy capacity increase is yielded.

The technique of filter hopping with FBMC is still in a preliminary phase before a practical use in a real system. This is mainly due to the limitations in filter design, which are still part of further research. However, with the promising initial results [46], the filter hopping technique might prove suitable for an enhanced secrecy in 5G physical layer applications.

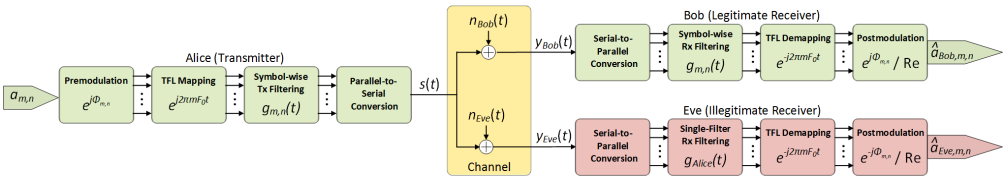

Fig. 8. FBMC filter hopping transmission chain with eavesdropper [46].

C. Physical layer key generation

Conventional symmetric key negotiation techniques, like the Diffie-Hellman key exchange [32] or techniques based on the RSA algorithms [63], were not specifically developed for wireless communications. They generally use a secret knowledge at both partner's (Alice's and Bob's) side and then negotiate a shared secret key (in case of Diffie-Hellman) over an authenticated public channel, or employ a public-private key pair for securely exchanging a shared secret (in case of RSA). The resulting key on both sides can then be used e.g. for symmetric encryption techniques. Instead of relying on the computational complexity of a mathematical problem in the case of conventional encryption techniques [64], [65], physical layer key generation techniques rely on the wireless channel as a common and reciprocal entropy source for Alice and Bob. The use of these novel techniques can both increase the security of a key exchange and also lower its complexity in comparison to conventional algorithms.

First considering the conventional techniques, the term *public* for the required public authenticated communication channel in the context of Diffie-Hellman means that an Eve can listen to the communication, e.g., by wiretapping the wireless connection or any other signal transmission technique inbetween. *Authenticated* means that the originators of negotiation messages for the key exchange are verified and the message is unchanged. Otherwise, MIM attacks could possibly compromise the security of the whole key negotiation. The authentication is a necessary prerequisite for the Diffie-Hellman key exchange, otherwise, such a MIM attack is possible. However, extensions and modifications of the Diffie-Hellman key exchange exist, which tackle this problem [66]. The conventional key exchange techniques are well-established, but also have several disadvantages, like complexity, the required key-distribution techniques with their dependencies, and their focus on the computational complexity of mathematical problems, based on specific functions as a barrier for the eavesdropper [48]. This is one of the reasons why physical layer key generation techniques emerge as an alternative or extension to the classical solutions.

The wireless communication channel as a reciprocal random source for both Alice and Bob can be realized by, e.g., using the channel impulse responses or received signal strength [49]. Important physical parameters for this are the mobility, the scattering of the environment and signal wavelength. Mobility is important for ensuring a significant variation of the channel in order to generate a sufficient amount of random data for generating and renewing the keys [64]. The signal wavelength λ, however, is relevant for the correlation of the channel state in comparison to a close-by position. If an eavesdropper has a distance higher than $\frac{\lambda}{2}$ to the key negotiation partners and the reflections of the environment are sufficiently scattered, he will not be able to extract the channel state information of the legitimate users [49].

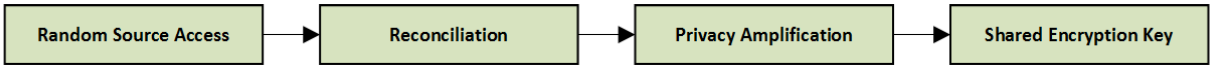

Fig. 9. Overview of physical layer key generation process.

An important aspect for secure communication on a public channel is feedback [52]. In contrary to the definition of Wyner's wiretap channel [10], where the eavesdropper is degraded (having a higher noise level) in comparison to the legitimate users for achieving secure communication, the author of [47] shows that with the so-called *public discussion*, an advantage over Eve can be gained. This finally allows a secret key negotiation even with an initial advantage of the Eavesdropper.

In the following, the practical structure of the physical layer key generation process is explained, which is also shown in Fig. 9. The first part of the process is the *random source access*, where the random source is the wireless channel, by accessing it via bidirectional transmissions. This can for example be done in a time-division duplexing (TDD) manner, if the channel variation is slow enough. The randomness extracted in this step can consist of characteristics like the channel impulse response or received signal strength [49]. This process is performed until both Alice and Bob have a sufficient amount of secure shared information. This also involves the so-called *advantage distillation* [48], which seeks to improve the secrecy advantage of Alice's and Bob's observations. For the channel as an entropy source, the authors of [67] presented two possible information-theoretic models, the *source-type* and the *channel-type model*. For the first, the channel is modeled as a discrete memoryless multiple source, which is basically independent of the communication participants and probed by all terminals. For the *channel-type model* in contrary, a discrete memoryless channel is used, which features an input from one communication partner and an output to both the other partner and the Eavesdropper. Here, the output depends on the input message, meaning that the input into the channel can be controlled by the transmitter, which is practically closer to the model of a real channel. In addition, both models feature the required noiseless public channel in parallel, which is necessary for the subsequent discussion process.

The second stage is the *reconciliation* stage. Here, a mutual agreement between Alice and Bob is achieved by eliminating error factors due to noise and imperfections, e.g. due to the type of the measurement [48], [49]. This can be done using error-correcting codes. The reconciliation may also inhere a partial revelation of information to the eavesdropper. For this reason, the so-called *privacy amplification* stage is carried out afterwards. It has the goal of eliminating the remaining information of Eve over the secret key agreement, which may be left due to the previous random source access and the reconciliation stages [49]. From the *leftover hash lemma* [50], [51], we can follow that a secure key can be yielded by using specific reductions functions (hash functions) in a compression process. They yield a close to uniform distribution if the input distribution is sufficiently compressed (with *sufficient*, the reduction by the whole amount of side-information of the eavesdropper is meant). Thus, we know that we can get a new key with a reduced length after the compression, where the remaining partial information from the eavesdropper is removed, and thus realize the *privacy amplification* process. This finally leads to the secure *shared encryption*

key.

As a conclusion, physical layer key generation is a promising technique for future wireless communications. It can be used as an alternative to conventional techniques, by shifting the secrecy paradigm from the computational complexity of trapdoor functions in current encryption techniques further to an information-theoretic level. Also, physical layer key generation can be used as an additional security measure to classical application layer encryption. By directly integrating it into the physical layer of the communication system, secrecy can already be reached on the lowest layer of the communication structure. Also, for miniature-type devices with power constraints, these techniques can be a promising alternative due to a possible complexity reduction. Still, more research is required to tackle the problem of a low key generation rate in slowly-varying channels [64]. Further information on the practical techniques for secure mutual key generation and distillation can be taken from the literature sources [47], [48], [52], [67].

D. Considerations on implementation in future mobile networks

The aforementioned techniques for physical layer security promise good results, however some of them come with some constraints which makes it hard for practical implementation. Interestingly, implementation of physical layer security systems are very limited to this date, as most of the physical security techniques require very high computational power for calculations.

Considering the battery life of mobile devices, it is more likely for these techniques will be implemented on the base station side first, hence the adaptive beamforming techniques are a good candidate for future implementation. Artificial noise and interference shaping based approaches increase secrecy, however there is more challenges when it comes to practical implementation, for example, it should be ensured that no legitimate user is bothered by the transmitted noise. These techniques should be tested and validated before considered as a practical approach.

However, with software defined radio (SDR) [68], it is possible to interoperate the radio components with high calculation power and change the radio parameters on the run. This ability is the first step that closes the gap between the research and practice in physical layer security systems. We have conducted a preliminary work in [69] where we show that the artificial noise technique is working in a real world scenario, and we intend to develop the test bed in order to pioneer the physical layer security implementation in the literature.

VII. Conclusion

As wireless technologies are a significant part of mobile networks, wireless security is very important for mobile networks of today and the future. In this chapter the wireless last mile of mobile networks is contextualized, discussing the advantages and disadvantages it brings. The security concerns regarding the usage of wireless technologies are covered. Main concepts of wireless systems and physical layer security are introduced and the relation between the wireless attacks and vulnerabilities are given. The current solutions for security are explained along with the future solutions. Here we can conclude that the current technologies are not sufficient to meet the security issues, however the future solutions are very promising. The concerns regarding the implementation of

those solutions are valid today and there may be some time needed before these techniques can be implemented in next generation mobile networks.

REFERENCES

[1] StatCounter, "StatCounter global stats," Jun 2015, online, Available: http://gs.statcounter.com/.

[2] C. Gonzales, "Mobile services business and technology trends," in *IEEE International Conference on Web Services*, Sept 2008, pp. 3–3.

[3] B. Durkin and I. Lokshina, "The impact of integrated wireless and mobile communication technologies on the corporate world," in *Wireless Telecommunications Symposium (WTS), 2015*, April 2015, pp. 1–5.

[4] M. Meeker, "Kleiner Perkins Caufield Byers 2015 Internet Trends," May 2015, online, Available: http://www.kpcb.com/internet-trends.

[5] P. Mandl, P. Schrotter, and E. Leitgeb, "Wireless synchronous broadband last mile access solutions for multimedia applications in license free frequency spectrums," in *6th International Symposium on Communication Systems, Networks and Digital Signal Processing*, July 2008, pp. 110–113.

[6] P. Mandl, E. Leitgeb, M. Loschnigg, T. Plank, and P. Pezzei, "FSO and WLAN as backward channel for internet connections of peripheral regions only covered by DVB-T," in *15th International Conference on Transparent Optical Networks (ICTON)*, June 2013, pp. 1–5.

[7] J. Proakis and D. Manolakis, *Digital signal processing*. Pearson Prentice Hall, 2007.

[8] V. Erceg, K. V. S. Hari, M. Smith, and D. S. Baum, "Channel models for fixed wireless applications," *Contribution to IEEE 802.16.3*, Jul. 2001. [Online]. Available: http://www.nari.ee.ethz.ch/commth//pubs/p/EHSB01

[9] M. Narandzic, C. Schneider, R. Thomä, T. Jämsä, P. Kyösti, and X. Zhao, "Comparison of scm, scme, and winner channel models," in *IEEE 65th Vehicular Technology Conference, VTC2007-Spring*. IEEE, 2007, pp. 413–417.

[10] A. D. Wyner, "The wire-tap channel," in *Bell System Technical Journal*, vol. 54, 1975, pp. 1355–1387.

[11] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339 – 348, may 1978.

[12] M. Sarkar and T. Ratnarajah, "Secrecy capacity and secure outage performance for Rayleigh fading SIMO channel," in *IEEE Int. Conf. on Acoust., Speech, Signal Process. (ICASSP)*, 2011, pp. 1900 –1903.

[13] S. Yang, P. Piantanida, M. Kobayashi, and S. Shamai, "On the secrecy degrees of freedom of multi-antenna wiretap channels with delayed CSIT," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2011, pp. 2866–2870.

[14] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in miso systems with partial channel information," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 704–716, 2012.

[15] J. Huang and A. Swindlehurst, "Robust secure transmission in miso channels based on worst-case optimization," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1696–1707, 2012.

[16] X. Yang and A. Swindlehurst, "On the use of artificial interference for secrecy with imperfect CSI," in *IEEE 12th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2011, pp. 476–480.

[17] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 3, pp. 901–915, 2011.

[18] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2840–2852, 2013.

[19] A. Mukherjee and A. Swindlehurst, "Ensuring secrecy in MIMO wiretap channels with imperfect CSIT: A beamforming approach," in *2010 IEEE International Conference on Communications (ICC)*, May. 2010, pp. 1 –5.

[20] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[21] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing,*, vol. 59, no. 3, pp. 1202 –1216, March 2011.

[22] X. Liu, F. Gao, G. Wang, and X. Wang, "Joint beamforming and user selection in multicast downlink channel under secrecy-outage constraint," *IEEE Communications Letters*, vol. 18, no. 1, pp. 82–85, January 2014.

[23] G. Dartman, O. Cepheli, G. Karabulut Kurt, and G. Ascheid, "Beamforming aided interference management with improved secrecy for correlated channels," in *Proc. IEEE 79th Vehicular Technology Conference - VTC'14-Spring, Seoul, Korea,*, May 2014.

[24] D. Ng, E. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4599–4615, Aug 2014.

[25] N. Romero-Zurita, D. McLernon, and M. Ghogho, "Physical layer security by robust masked beamforming and protected zone optimisation," *IET Communications*, vol. 8, no. 8, pp. 1248–1257, May 2014.

[26] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. on Info. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[27] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. on Info. Theory*, vol. 54, no. 6, pp. 2515 –2534, June 2008.

[28] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE Int. Symposium on Information Theory*, july 2006, pp. 356 –360.

[29] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *IEEE Int. Symp. on Information Theory*, 2007, pp. 1301–1305.

[30] P. Singer and A. Friedman, *Cybersecurity: What Everyone Needs to Know*. Oxford University Press, USA, 2014.

[31] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *INFOCOM, 2011 Proceedings IEEE*, April 2011, pp. 1871–1879.

[32] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov 1976.

[33] A. George and M. Kiesler, "Secret communication system," Aug. 11 1942, uS Patent 2,292,387.

[34] B. Gaston, "Applications of spread spectrum radio technology for the security market," in *IEEE 28th Annual 1994 International Carnahan Conference on Security Technology*, Oct 1994, pp. 86–91.

[35] R. Ziemer and R. Peterson, *Digital communications and spread spectrum systems*. Macmillan, 1985.

[36] S. M. Schwartz, "Frequency hopping spread spectrum (fhss) vs. direct sequence spread spectrum (dsss) in broadband wireless access (bwa) and wireless lan (wlan)," http://sorin-schwartz.com/white_papers/fhvsds.pdf.

[37] T. Li, J. Ren, Q. Ling, and A. Jain, "Physical layer built-in security analysis and enhancement of cdma systems," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, Oct 2005, pp. 956–962 Vol. 2.

[38] F. Hermanns, "Cryptographic CDMA code hopping (CH-CDMA) for signal security and anti-jamming," in *Proceedings EMPS 2004*, 2004.

[39] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for cdma systems," *EURASIP J. Wirel. Commun. Netw.*, vol. 2007, no. 3, pp. 7:1–7:16, Jul. 2007.

[40] J. Zhang and M. Gursoy, "Relay beamforming strategies for physical-layer security," in *2010 44th Annual Conference on Information Sciences and Systems (CISS)*, March 2010, pp. 1 –6.

[41] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing,*, vol. 59, no. 3, pp. 1202 –1216, March 2011.

[42] S.-H. Lai, P.-H. Lin, S.-C. Lin, and H.-J. Su, "On optimal artificial-noise assisted secure beamforming for the fading eavesdropper channel," in *IEEE PIMRC*, sept. 2011, pp. 1167 –1171.

[43] G. Dartmann, X. Gong, W. Afzal, and G. Ascheid, "On the duality of the max-min beamforming problem with per-antenna and per-antenna-array power constraints," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 2, pp. 606–619, Feb 2013.

[44] X. Gong, M. Jordan, G. Dartmann, and G. Ascheid, "Max-min beamforming for multicell downlink systems using long-term channel statistics," in *IEEE PIMRC*, 2009, pp. 803–807.

[45] G. Dartmann, V. Lucken, O. Cepheli, G. K. Kurt, and G. Ascheid, "Filter optimization aided interference management with improved secrecy," in *IEEE Vehicular Technology Conference (VTC Fall)*, Sept 2014, pp. 1–6.

[46] V. Luecken, T. Singh, O. Cepheli, G. Karabulut Kurt, G. Ascheid, and G. Dartmann, "Filter hopping : Physical layer secrecy based on fbmc," in *IEEE Wireless Communications and Networking Conference , New Orleans, LA, USA*, March 2015.

[47] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[48] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[49] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, June 2015.

[50] M. Petkovic and W. Jonker, *Security, Privacy, and Trust in Modern Data Management*, ser. Data-Centric Systems and Applications. Springer, 2007.

[51] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, ser. STOC '89. New York, NY, USA: ACM, 1989, pp. 12–24.

[52] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Taylor & Francis, 2013.

[53] J. Zhu, X. Jiang, Y. Zhou, Y. Zhang, O. Takahashi, and N. Shiratori, "Outage performance for secure communication over correlated fading channels with partial CSI," in *Services Computing Conference (APSCC), 2012 IEEE Asia-Pacific*, 2012, pp. 257–262.

[54] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in mimo wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, 2011.

[55] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Sig. Proc. Letters*, vol. 20, no. 1, pp. 39–42, 2013.

[56] X. He and A. Yener, "Providing secrecy irrespective of eavesdropper's channel state," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, 2010, pp. 1–5.

[57] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628 –1631, Oct. 2012.

[58] S. Bayat, R. Louie, Z. Han, B. Vucetic, and Y. Li, "Physical-layer security in distributed wireless networks using matching theory," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 5, pp. 717–732, 2013.

[59] M. Ghogho and A. Swami, "Characterizing physical-layer secrecy with unknown eavesdropper locations and channels," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2011, pp. 3432–3435.

[60] S. Anand and R. Chandramouli, "On the location of an eavesdropper in multiterminal networks," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 1, pp. 148–157, 2010.

[61] S. Goel, V. Aggarwal, A. Yener, and A. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2010, pp. 2627–2631.

[62] M. Schellmann, Z. Zhao, H. Lin, P. Siohan, N. Rajatheva, V. Luecken, and A. Ishaque, "FBMC-based air interface for 5G mobile: Challenges and proposed solutions," in *9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, June 2014, pp. 102–107.

[63] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[64] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *IEEE INFOCOM Proceedings*, April 2011, pp. 1125–1133.

[65] Z. Hao, S. Zhong, and L. Li, "Towards wireless security without computational assumptions; an oblivious transfer protocol based on an unauthenticated wireless channel," in *IEEE INFOCOM Proceedings*, April 2011, pp. 2156–2164.

[66] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Des. Codes Cryptography*, vol. 2, no. 2, pp. 107–125, Jun. 1992.

[67] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Jul 1993.

[68] E. Grayver, *Implementing software defined radio*. Springer Science & Business Media, 2012.

[69] O. Cepheli and G. Kurt, "Analysis on the effects of artificial noise on physical layer security," in *Signal Processing and Communications Applications Conference (SIU), 2013 21st*, April 2013, pp. 1–4.