A Survey on Secret Key Generation Mechanisms on the Physical Layer in Wireless Networks

Youssef El Hajj Shehadeh, Dieter Hogrefe
Institute of Computer Science, University of Goettingen, Germany.

ABSTRACT

Traditional security mechanisms are mainly based on the distribution of shared secret keys. Yet, this task is non trivial in large wireless networks, due to mobility and scalability issues. Recently, it has been found that some properties of the physical layer of wireless communications can be leveraged for the purpose of secret key generation. In particular, the wireless channel has been investigated as a common source of secrecy to generate a shared secret key. We explore the most recent approaches in this area. RSSI-based key generation is firstly investigated. After that, we present some of the most recent approaches of key generation based on the channel impulse response. Moreover, we discuss some other physical layer methods. Thus, this paper provides a survey on the latest key generation mechanisms on the physical layer of wireless communications. Copyright © 2013 John Wiley & Sons, Ltd.

KEYWORDS
Physical-layer security; key generation; wireless multipath channel; RSSI; CIR

1. INTRODUCTION

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

In fact, one of the main requirements of communication security is the distribution of secret keys between communicating nodes. Some traditional solutions consider Public Key Infrastructure (PKI) mechanisms for key exchange [1] in the presence of a Certification Authority (CA). But PKI mechanisms are only computationally secure and require high computational complexity. In addition, the requirement of having a CA makes these solutions unpractical in some scenarios, mainly in Ad hoc and sensor networks.

Other solutions consider key predistribution schemes (see for example [2]). However, key predistribution schemes lack scalability which makes them inappropriate especially in case of large-scale sensor deployments or mobility. As a result, there have been recently many efforts to find other ways to secure wireless communications.

In optical communications, quantum cryptography [3] has been largely investigated as a security solution based on the uncertainty principle in quantum physics. As for wireless communications, the wireless multipath channel has appeared recently to be a candidate. In deed, a lot of attention is being given to the physical layer of wireless communication and physical layer security has become an active area of research in the last decade.

The idea of generating keys based on the characteristics of the radio channel was first introduced by Hassan et al. in their pioneering work in [4]. Since then, many efforts have been invested in generating secret keys on the physical layer. Many of these efforts have investigated generating keys using functionalities provided by current of-the-shelf devices. These are mainly based on quantizing the RSSI (Received Signal Strength Indicator). This parameter is provided by the physical layer based on calculating the average received signal power over a certain period. They also consider a Reconciliation stage to enhance the reliability of the extracted key, and finally a Privacy Amplification stage to enhance the secrecy. These approaches were validated by practical implementations and measurements using of-the-shelf devices or Universal Software Radio Peripherals (USRP) [5, 6, 7].

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

Indeed, channel-phase based quantization methods have three major advantages. First, the uniform distribution of the phases of the channel taps implies a higher level of secrecy [8]. Second, a higher secret key generation rate can be achieved by leveraging the whole channel impulse response and quantizing the phases of the different channel taps. Third, this allows a spontaneous key extraction, as it is only required to have an estimate of the channel impulse response at a certain instance instead of needing to estimate the average received power over a certain time window. However, RSSI-based approaches have the advantage of being implementable in most off-the-shelf devices, and therefore they do not need significant hardware modifications. In fact, RSSI is usually available to the higher layers in most wireless transceivers. In addition to that, RSSI based schemes are more robust to synchronization issues.

For a theoretical comparison of the key generation rates based on CSI and on RSSI, the reader is advised to read [9]. The authors of [9] derive the secret key capacity in case of CSI quantization and in the case of RSSI quantization and prove the superiority of the former one.

In this paper, we review these two approaches and show a summary of the recent related work on each. But firstly, we present information theoretic studies in this area. Actually, there have been many more generic approaches investigating generating secret keys from correlated sources of randomness. We also review reconciliation and privacy amplification, as these steps are essential in many proposed key extraction and agreement methods. After that, we review in section II the latest approaches of generating secret keys based on RSS measurements. In section III, we discuss the latest CIR-based attempts to generate secret keys. In section IV, some other methods for generating secret keys on the physical layer are summarized. Finally, we conclude this survey in section V with a summary and conclusions.

1.1. Information-Theoretic Perspective

From an information-theoretic point of view, many authors [10, 11, 12] explore the possibility of generating secret keys from correlated sources of randomness.

Maurer in his pioneering work in [10], demonstrates that it suffices for two nodes to be in access to a common source of information, observed differently by other nodes, to achieve perfect cryptographic security regardless of the enemy’s computing power. He actually defines the notion of secret key rate and derives upper and lower bounds on the achievable size of the generated key.

![Figure 1. Types of physical layer key generation mechanisms.](image-url)

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

$$S(X; Y | Z) \leq \min[I(X; Y)], \min[I(X; Y | Z)] \tag{1}$$

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

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

$$S(X; Y | Z) \geq \max[I(Y; X) - I(Z; X), I(X; Y) - I(Z; Y)] \tag{2}$$

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

1.2. Reconciliation

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

**Information reconciliation**, also referred to as public feedback or error correction, is the process of detecting and correcting errors by public discussion targeting a higher probability of agreement between the derived keys. It is mainly based on the exchange of syndromes and/or parity check bits and the application of an error correcting code [14, 15, 16].

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

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

### 1.3. Privacy Amplification

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

To cope with this problem and distill perfect secret keys, privacy amplification [17, 18] is necessary. This can be achieved by using universal hash functions [18, 19, 20, 21], or by using extractors [21, 22, 23, 24, 25].

## 2. RSSI-BASED KEY GENERATION

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

In [26], Mathur et al. used a two-level crossing excursion-based quantization algorithm to extract bits from CIR and RSS measurements. They evaluated their algorithm through theoretical and numerical studies providing important insights on the appropriate probing rate and the quantization parameters. Further, they validated their proposed algorithm through experiments using an IEEE 802.11 development platform. Two approaches were considered, one based on the channel impulse response and the other based on the received signal strength indicator. In their experiments, the CIR was extracted per-packet basis from the preamble of a format-compliant 802.11a packet which makes their approach equally applicable to off-the-shelf 802.11 hardware. On the other hand, they used off-the-shelf devices to collect coarse RSS measurements. In both approaches, they showed by experiments that it is possible to practically achieve key establishment rates of $\approx 1$ bit/sec at an infinitesimally small error probability in an indoor wireless environment.

This algorithm was further improved in [27, 28, 29]. In [27], an over-quantization method was included followed by a reconciliation stage and finally a privacy amplification stage. The authors apply a $1/2$ rate LDPC (Low Density Parity Check Code) code with error correcting based on the exchange of log likelihood ratio estimates to achieve an improved secret key generation rate of $10$ bits/sec.

Similarly, in [28, 29], Jana et al. propose an adaptive scheme to extract multiple bits from a single RSS measurement. They also include information reconciliation to remove any discrepancies between the extracted bits, and finally apply a privacy amplification mechanism to the reconciled bits to obtain a higher entropy bit stream. The authors perform extensive real world measurements in different scenarios and settings and discuss the effectiveness of RSS-based secret key extraction. Moreover, in [29], the authors investigate key extraction in MIMO (Multiple Input Multiple Output) systems. They consider a MIMO-like sensor testbed and perform RSS measurements to extract secret keys. To enhance the performance of their mechanism and decrease the bit mismatch rate especially in MIMO systems, they introduce an iterative distillation step before the information reconciliation stage. It is mainly based on eliminating measurements that are likely to lead to mismatched bits at Alice and Bob.

In [30], Patwari et al. introduced a framework for the extraction of secret bits from a series of radio channel measurements, called HRUBE (High Rate Uncorrelated Bit Extraction). The framework includes 3 main steps: interpolation, transforming for decorrelation, and a multibit adaptive quantization method. The authors argue...
that it is not practically possible in most transceivers to obtain simultaneous channel measurements due to the half-duplex nature of the wireless communication. Therefore, the authors tend to collect channel samples at some instants and use fractional interpolation filtering to allow nodes to estimate what the measurements would have been if they have been made simultaneously. After that, they propose a Karhunen-Loeve transform (KLT) to convert the obtained channel vectors into uncorrelated components. As for the quantization, the authors propose an adaptive quantization scheme achieving a higher efficiency than the usual censoring (or guard-intervals) scheme. They provide an analysis of the probability of bit disagreement in the generated secret keys and perform an experimental implementation in Crossbow telosB wireless sensor nodes. Their experimental results showed that the implemented HRUBE system can achieve a secret key generation rate of 22 bits/sec at a bit disagreement rate of 2.2 percent, or 10 bits/sec at a bit disagreement rate of 0.54 percent.

Based on the HRUBE framework, a more robust bit extraction method, called ARUBE (Adaptive Ranking-based Uncorrelated Bit Extraction) has been proposed in [31]. It reduces the non-reciprocities caused by different hardware characteristics by including a ranking step after the interpolation filtering. Compared to the HRUBE extraction method, this method is more robust to differences in hardware, adapts to the channel environment, can be implemented in wireless motes, and produces, for medium and high SNR channels, 30% – 60% more bits per sample with a low probability of bit disagreement. Indeed, the tested method has proven to be able to extract 40 bits/sec at a probability of bit disagreement of 0.04 percent.

On the other hand, Azimi-Sadjadi et al. have followed a different approach to quantize the RSS values [32]. Their approach is mainly based on quantizing the deep fades in the received signal. Consequently, a measurement is encoded as a 0 if it is lower than a deep fade threshold and 1 otherwise. They argue that this method is more robust to non-reciprocities between the channel measurements. Moreover, they proposed a method to enhance the entropy of the extracted bit stream, called secure fuzzy information reconciliation. It is mainly based on using fuzzy extractors which are characterized by their error correction capability in addition to privacy amplification [33]. However, the reliance on deep fades to extract secret bits results in a relatively low secret key generation rate.

In [34, 35], Wilhelm et al. validated the correlation of measured RSSI values by performing measurements using MICAz sensor nodes. The authors developed a key generation mechanism based on RSSI measurements provided by the sensor nodes. They have considered leveraging the multiple available channels and applying multi-level quantization to increase the key generation rate. Moreover, to increase the error tolerance, they have considered collecting a number of samples and calculating their average value. They have also applied information reconciliation by using an error correcting code and the transmission of a public reconciliation code providing information about the distance of the derived key to the nearest codeword. Consequently, privacy amplification was applied by using randomness extractors and universal hash functions.

Using higher bandwidths and multiple channels in the frequency domain to enhance the secret key generation rate has been also investigated in [36]. In this paper, Forman et al. consider a 200MHz bandwidth divided into 80 different and independent subchannels. Consequently, they tend to quantize the normalized amplitude and phase of the subcarriers to generate secret keys.

Channel reciprocity was also validated in UWB (Ultra Wide Band) communication systems [37]. In this paper, the authors perform a two level quantization of the received signal strength to generate a secret key.

Apart from that, some works tackle the problem of generating secret keys in stationary channels [38, 39, 40, 41]. In [38], Aono et al. investigate using ESPAR (Electronically Steerable Parasitic Array Radiator) antenna to create artificial fluctuations of the channel characteristics. Their method is mainly based on fluctuating the channel characteristics intentionally using beamforming techniques of the ESPAR antenna. Hence, more randomized and stronger keys can be extracted using this innovative technique thus achieving a higher secret bits extraction rate. Indeed, using their proposed scheme, multiple channel probing packets can be transmitted consecutively even in stationary channels, each with a different random beamform vector used during the transmitting and receiving phase at the access point. Whereas the user terminal is associated with an omni-directional antenna. In addition, the authors target a high probability of key agreement by probing the channel multiple times and then choosing the best RSSI measurements by public discussion and agreement between the two parties. They further enhance the reliability of the key generation mechanism by applying error correction using a BCH error correcting code. Finally, key verification is accomplished by using a one-way hash function. Experiments in different scenarios using ZWigBeeTM chips were performed to validate the proposed key generation mechanism.

An improvement to this key generation mechanism was proposed in [39]. It is mainly based on including an RSSI interleaving scheme which enables to acquire more randomized and stronger secret keys. The authors have also conducted experiments based on ZigBeeTM chips to validate their key generation mechanism. Experimental results showed that a probability of success of 99.998% would be obtained when 128-bit secret keys are exchanged every two seconds. They also verified the secrecy of the derived keys by applying the FIPS (Federal Information Processing Standards) PUB 140-2 [42] statistical test for random numbers.

This method was further improved in [41] by applying a multi-level quantization to increase the key extraction rate.
However, these approaches require special antennas which make them non-ubiquitous and expensive solutions.

In addition, many works have considered leveraging multiple antennas to enhance the key generation rate. Actually, Zeng et al. were one of the first to investigate key generation in real multiple-antenna wireless systems [43]. In their paper, they consider quantizing RSSI measurements at multiple antennas and applying multi-level quantization. They consider using guard intervals and excursion-based quantization to reduce the probability of error. Their method includes a public discussion phase consisting of agreement on the antennas to be used, the quantization levels, the excursion size, the guard interval, and the RSSI measurements to be quantized. Further, they apply a simple bit-wise xor function as a privacy amplification scheme to increase the entropy of the derived key.

In [40], a new scheme using multiple antennas is proposed where a common private key is generated based on the variation produced by antenna switching. In this scheme, Kitiura et al. propose to compare the signal strength at two antennas to generate a secret key instead of using the conventional threshold method.

It is also interesting to study the channel probing rate for the purpose of key generation. In this realm, it is important to consider the pioneering work of Wei et al. in [44] where a relationship between the optimal probing rate and the bit extraction rate is derived. The authors develop a mathematical model of channel probing and argue that channel probing should not be too fast to achieve a desirable extraction rate; but only fast enough to avoid using the channel inefficiently. They propose a scheme based on Lempel-Ziv complexity to estimate the entropy rate of the channel statistics and they use a Proportional-Integral-Derivative (PID) to adjust dynamically the probing rate to achieve the desired secret key generation rate.

More recently, Zan et al. have investigated the robustness of key extraction against active attacks [45]. In their paper, they consider the case of a physically-active attacker capable of provoking small fluctuations in the wireless environment. They propose a differential technique to quantize the RSS measurements and a moving average to remove the effect of small predictable fluctuations and enhance the security of the derived key.

Liu et al., in [46], discuss the reliability of quantization using thresholds and propose a fading trend key generation mechanism based on transforming the trend of the RSS to bits instead of the usual threshold quantization. In addition, they introduce a relay node assisted scheme for key generation between nodes which are not in the transmission range of each other. However, the security of this scheme relies on the trustworthiness of the relay node.

These approaches emphasize the possibility of generating secret bits from the wireless channel. However, they are still far from what can be achieved due to the hardware limitations of the considered off-the-shelf devices.

Therefore, other efforts have investigated bit extraction mechanisms based on the whole channel impulse response. We summarize some of these recent approaches briefly in the next section.

3. CIR-BASED KEY GENERATION

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

In this context, Wilson et al. were one of the first to derive the secret key capacity in multipath channels. In their pioneering work [47], they derive an expression of the mutual information between the channel observations, which forms an upper bound on the secret-key rate. They also investigate the variation of this rate as a function of the signal bandwidth. Interestingly, it was found that the secret-key rate does not increase monotonically with bandwidth. Consequently, the optimal signaling bandwidth as a function of SNR for some typical UWB channel excess delays is derived. In addition, the authors have investigated different public discussion methods and compared them through simulations.

Chunxuan et al. were also one of the first to investigate key extraction from multipath channels. In [48], they investigate key generation from jointly Gaussian random variables and derived the secret key capacity as a function of the received SNR. In addition, the authors propose a key generation mechanism based on applying an equally probable quantization scheme and an LDPC error correcting code for error reconciliation. Furthermore, they also compare gray coding and natural coding.

In [49], this key generation algorithm is further extended and applied on ITU channels [50]. In fact, wireless channel taps have been shown to have a complex Gaussian distribution [8]. Therefore, the authors have applied their approach on multipath wireless channels. They propose an Orthogonal Greedy Algorithm (OGA) for channel decomposition and extraction of channel taps. Then, they apply the quantization and error correction techniques in [48] to validate the key generation efficiency from typical multipath fading channels.

In [51], Sayeed et al. consider a simple block fading model where the frequency band is divided into D coherence bands. The authors consider the phase quantization of the channel coefficients in the different
frequency bands which were supposed to be independent and identically distributed. The main contribution of this paper is the derivation of the probability of error as a function of SNR and the number of quantization levels. The authors also derive the minimum energy required for a successful acquisition of a secret key between two nodes.

In [52], Wallace investigates the theoretical limits of the secret key rate from multipath wireless channels in case the channel at the eavesdropper is correlated with that at the legitimate nodes. The author derives the secret key rate in function of the channel covariance matrices. Interestingly, it was found that from a security perspective channels with higher order of diversity (higher number of paths) are more suitable for secret key generation. Moreover, an intelligent Channel Quantization mechanism with Guard bands (CQG) is proposed in this paper. It is mainly based on mitigating errors by the separation of the decision areas by guard bands.

This mechanism was further investigated in [53, 54]. In [53], Sun et al. analyze the performance of the CQG mechanism and derive expressions for the Bit Error Rate (BER) and the key generation efficiency. Moreover, the authors consider concatenating this protocol with reconciliation viewed as a Slepian-Wolf lossless compress coding [55]. They show that the key generation efficiency can be maximized by selecting appropriate guardband regions and LDPC code rates. Moreover, the optimal quantization and guardband parameters for the CQG mechanism are derived in [54].

In [56, 57], an intelligent key generation mechanism called “Channel Quantization Alternating (CQA)” was proposed. It is mainly based on using alternating staggered quantization maps instead of a guard band. Using simulations, this method has been proven to achieve a better performance than the direct quantization and the quantization with guard band methods. Furthermore, the authors discuss the case of multi antennas and investigate different rate error correcting codes.

Shehadeh et al. propose another intelligent key generation mechanism called Phase Shifting (PS) in [58]. It is mainly based on shifting the phases of the channel taps synchronously toward the constellation points without any loss of secrecy. In this paper, the authors show that this method achieves a higher secret key generation rate even at a low probability of disagreement. Moreover, some practical issues that affect the reliability of key generation from wireless channels are investigated in [59]. The authors mainly consider delay and mobility and propose an efficient and robust key generation mechanism. Interestingly, they also show that mobility can be an advantage to the key generation procedure.

Alternatively, a different attempt has been proposed by Chen et al. in [60, 61]. In this work, the authors propose a MIMO-channel based encryption of a channel matrix, to be used to generate a secret key. Further the authors discuss several error reduction techniques such as Gray coding, least-square estimation, channel averaging and LDPC codes.

In [62], a new method has been proposed for generating secret keys based on the common wireless channel. In this work, the authors do not quantize directly the phases of the channel taps. Instead, they consider sending random-phased beacons. These are then received at the legitimate node shifted by the random phase of the common channel. In other words, it is a kind of channel encryption of a chosen random phase value which will be consequently used to derive a secret key. Moreover, the authors propose using the channel multiple times even during the coherence period to achieve a high secret key generation rate. However, this method is not secure and any adversary in the communication range of the two nodes is able to deduce a correlation between the bits of the agreed-on key.

In addition to that, a relay-assisted scheme for key generation is proposed in [63, 64]. In this scheme, multiple relay nodes are employed to help increase the key generation rate. The authors derive expressions of the mutual information in addition to a more tight Cramer-Rao bound on the key rate. However, the security of such mechanism relies completely on the trustworthiness of the relay nodes.

Apart from that, Chou et al. [65] have studied the impact of channel sparsity and correlated eavesdropping on secret key generation from multipath wireless channels. In this work, the authors define a sparsity parameter \(\rho\) as the ratio of the subchannels having a non-vanishing independent coefficient, over the whole number of subchannels. Consequently, the authors derive the optimal sparsity that yields the maximum secret key capacity for a given transmitted SNR. Moreover, they tackle the issue of a correlated eavesdropper and investigate the effect of correlation with an eavesdropper’s channel measurements on the secret key capacity.

As for the case of Frequency Division Duplex (FDD) systems, key generation from the wireless multipath channel was investigated by Wang et al. in [66]. In their paper, the authors argue that despite the non-reciprocity of the channel impulse response, some parameters can be used for generating a common secret key. They consider that the multipath angles and the time delays of the multipath components are reciprocal parameters that can be used in generating secure keys. Consequently, they propose a key generation mechanism based on quantizing these parameters. Moreover, they propose a reconciliation stage by performing error correction based on the Chinese Remainder Theorem (CRT).

### 4. MISCELLANEOUS KEY GENERATION MECHANISMS

Apart from the channel impulse response or the received signal strength, there have been several other approaches proposed to generate secret keys based on some properties...
of the physical layer of wireless communication. Kitano et al. [67] have investigated secret key generation based on the fluctuations of the BER in wireless communications. The authors argue that BER is an appropriate indicator to characterize the wireless channel as it incorporates the different factors that lead to bit errors, such as fluctuations of amplitude and phase, and the effect of multipath and delayed waves.

Tsouri et al. [68] have proposed a reverse piloting protocol. The main idea of this protocol is the transmission of pilot signals by the receiver only so that the transmitter can estimate the channel and compensate it during the transmission through a coding scheme. As a result, the channel performs an automatic symbol level encryption. Further, the authors analyze this key generation mechanism and derive the relation between the efficiency of the source, the coherence bandwidth and the Doppler bandwidth. As for the secrecy of this protocol, the authors argue that an eavesdropper cannot have an accurate estimate of the channel and can only perform blind estimation since the transmitter does not send any pilots or reference signals. However, any known transmitted message (for example the synchronization signal) can be leveraged by the eavesdropper to estimate the channel and break the secrecy of the derived key. Therefore, this protocol needs further investigation to demonstrate its security.

A random channel hopping scheme for key agreement in wireless networks has been proposed by Zan et al. in [69]. In this scheme, the transmission of data is based on choosing a random hopping sequence. On the other hand, the receiver also listens on a random chosen channel; and when it hears a packet, it sends an acknowledgment. Hence, the received bit pattern will be used to establish a key. The authors have analyzed this approach and derived the average number of trials to reach key agreement and elaborated the probability of error of an adversary. However, the security of this mechanism is based on the assumption that the adversary is not able to listen to all channels simultaneously. Therefore, this key generation mechanism is not secure against a powerful adversary.

Gollakota et al. [6] have proposed a channel independent method for secret key agreement based on reactive jamming by the receiver. The method called iJam works as follows: The transmitter transmits 2 OFDM symbols while the receiver jams randomly half the time samples of each so that an eavesdropper will get a jammed signal. On the other hand, the jamming receiver knowing the jamming sequence will combine the non jammed samples to get a jamming-free OFDM symbol. The authors have further investigated different modulations and enhanced the effectiveness of this mechanism against eavesdroppers in different locations making their mechanism location independent. Finally, the results of their tested implementation showed that their design has a secrecy rate of 3 → 18 Kbps with a 0% bit disagreement.

5. SUMMARY AND CONCLUSIONS

We have summarized in this paper the latest proposed approaches for key generation and agreement on the physical layer of wireless communications. Some of the latest proposed RSSI-based key generation mechanisms were firstly reviewed. These target mainly key generation on the physical layer using of-the-shelf devices. However, RSSI-based key generation mechanisms suffer from relatively low secret bit extraction rates. After that, we have investigated the latest approaches based on CIR. These approaches show that leveraging CIR, a higher secret bit extraction rate is achievable. However, CIR-based key generation necessitates advanced channel estimation methods and high frequency and time synchronization. Finally, some other physical layer key generation methods were also summarized.

All the proposed mechanisms show that secret key generation on the physical layer is indeed possible. Yet, more investigations need to be done to verify the security of these systems. As for CIR-based key generation mechanisms, further work needs also to be done to verify these mechanisms in real implementations.

REFERENCES


42. 140-2 FP. Security Requirements for Cryptographic Modules 2002.


50. User equipment (ue) radio transmission and reception (ffd) (release 6) 2005.


