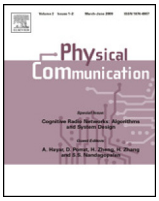
Physical Communication 19 (2016) 1–10

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom



Unleashing the secure potential of the wireless physical layer: Secret key generation methods

Ahmed Badawy[a,*], Tarek Elfouly[b], Tamer Khattab[c], Amr Mohamed[b], Mohsen Guizani[b]

[a] *Politecnico di Torino - DET, Italy*

[b] *Qatar University, Electrical Engineering Department, Qatar*

[c] *Qatar University, Computer Engineering Department, Qatar*

ARTICLE INFO

Article history:
Received 5 June 2015
Received in revised form 16 November 2015
Accepted 17 November 2015
Available online 16 January 2016

Keywords:
Physical layer security
Wiretap channel
Common source of randomness
Secret key generation
Secret key evaluation

ABSTRACT

Within the paradigm of physical layer security, a physical layer characteristic is used as a common source of randomness to generate the secret key. This key is then used to encrypt the data to hide information from eavesdroppers. In this paper, we survey the most recent common sources of randomness used to generate the secret key. We present the steps used to extract the secret key from the estimated common source of randomness. We describe the metrics used to evaluate the strength of the generated key. We follow that with a qualitative comparison between different common sources of randomness along with a proposed new direction which capitalizes on hybridization of sources of randomness. We conclude by a discussion about current open research problems in secret key generation.

1. Introduction

The broadcast nature of wireless communications imposes the risk of information leakage to adversarial users or unauthorized receivers. Therefore, information security between the intended users remains a challenging issue. Currently, wireless security relies on cryptographic techniques and protocols that lie at the upper layers of the wireless network. One main drawback of these existing techniques is the necessity of a complex key management scheme in the case of symmetric ciphers and high computational complexity in the case of asymmetric ciphers. Cryptographic techniques mandate the exchange of encryption keys at one point during the encryption—decryption process. This poses a serious threat to the secrecy of the whole communication session (i.e., becomes a security bottleneck). Minimization of the security risk, stemming from key exchange mechanisms, is the main reason that cryptographic secrecy opts for key reuse (i.e., using the same key for multiple packet encryptions), which introduces another secrecy weakness allowing an eavesdropper to have more chances on guessing the encryption key. Physical layer security relies on randomness characteristics inherent in the communication channels, which are common to the two trusted parties, which being unknown to a potential eavesdropper. Thus, key exchange is no longer mandatory and key renewal is potentially possible for every packet transmission rendering the secrecy potential higher than upper layers cryptographic methods while maintaining lower computational complexity [1].

The wiretap channel, first presented by Wyner in 1975 [2], models two legitimate nodes communicating through a noisy channel and an adversary receiving a deteriorated version of the exchanged signals between the

[*] Corresponding author.

E-mail addresses: ahmed.badawy@polito.it (A. Badawy), tarekfouly@qu.edu.qa (T. Elfouly), tkhattab@qu.edu.qa (T. Khattab), amrm@qu.edu.qa (A. Mohamed), mguizani@qu.edu.qa (M. Guizani).

http://dx.doi.org/10.1016/j.phycom.2015.11.005

legitimate parties through a wiretap channel. The paper studied the maximum secured transmission rate between the two legitimate nodes while minimizing the amount of information leaked to the wiretapper, i.e., eavesdropper. The paper concluded that an ‘approximately perfect’ secret communication between the two legitimate nodes is achievable up to a specified rate without the use of secret keys. This paper presented the early studies on the theoretical aspects of physical layer security.

In relatively recent literature [3–5], researchers started to exploit the randomness in some physical layer characteristics as a potential source for key generation to guarantee information hiding from eavesdroppers or in other words bound the amount of information leaked to unauthorized nodes. These physical layer characteristics have to be common to the two legitimate nodes and not shared with the adversarial users. In other words, an estimation of this physical layer characteristic should be approximately the same if measured from the receivers of either of the legitimate nodes. In addition, the physical layer characteristic used to generate the secret key should be randomly changing. Hence, the physical layer characteristic is also referred to as a *common source of randomness*.

Typically, in the wiretap channel paradigm, the adversary (i.e., eavesdropper), *Eve*, can listen to all communications between the two trusted parties (i.e., communicating nodes), *Alice* and *Bob*. Eve can estimate the channel between itself and both Alice and Bob. In addition, it can estimate the distances between itself and Alice and Bob. Eve can move freely within the field and can visit any of the locations where either Alice or Bob was or will be in the future. Eve, however, cannot be in very close proximity (i.e., within few wavelengths) to either Alice or Bob to ensure that the collected signals are not correlated.[1] There is no limitation on the number of the antennas Eve is equipped with nor its computational capabilities. It is assumed that Eve is not capable of pursuing denial of service attack, person in the middle attack or jamming attack.[2] Therefore, we assume that Eve is a passive adversary.

The objective of this survey is to present the fundamentals of secret key generation in an explicit way. The flow of the paper is organized as follows. In Section 2, we survey the most common physical layer characteristics used as common sources of randomness to generate the secret key. The steps used to extract the key from the estimated physical layer characteristic are presented in Section 3. We then present the metrics used to evaluate the strength of the secret key in Section 4 followed by a discussion in Section 5. The paper is concluded in Section 6.

2. Common sources of randomness

Fig. 1 depicts a typical system model for a secret key generation system. Several characteristics of the physical layer link between the two communicating nodes are shared between the two legitimate nodes, while the eavesdropper can only measure them between itself and between both nodes.

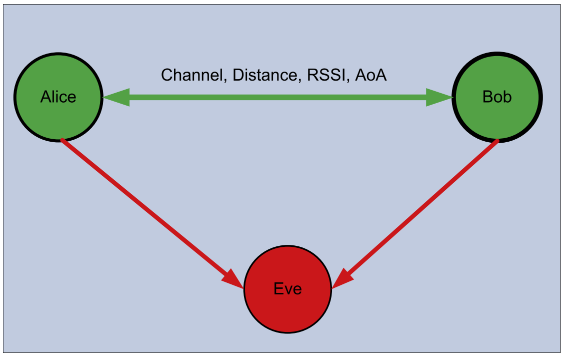


Fig. 1. System model.

2.1. Channel estimates

One well known characteristic of the communication channel is reciprocity. When two antennas communicate by radiating the same signal through a linear and isotropic channel, the received signals by each antenna will be identical. This is mainly because of the reciprocity of the radiating and receiving antenna pattern.

Current physical layer security techniques are based on channel reciprocity assumption. One of the pioneering work on secret key generation based on channel reciprocity was first presented in [3]. They concluded that the maximum size of the generated secret key mainly depends on the mutual information between the channel estimates at the two legitimate nodes. They also derived an expression for the mutual information for a general multipath channel. The most common feature of the channel characteristics that is widely used is channel gain; mainly because of its ease of implementation [6,7]. In [6], the authors studied the channel probing rate effect on the secret key rate for different doppler shifts. They found that secret key rate increases as the probing rate increases and saturates at 20 kHz probing rate for the worst case doppler shift they assumed of 100 Hz. The smaller the doppler shift the smaller the probing rate required to saturate the secret key rate. In [7], the authors observed that as the carrier frequency increases, the probing rate should increase to achieve a suitable key rate. This is mainly because the channel’s temporal variation increases at higher carrier frequencies.

Others exploit the channel phase to generate the secret key as in [8–10]. Unlike the channel gain, the channel phase is uniformly distributed in narrowband fading channels. The authors in [8,9], which were published in 1996 and 1998, respectively, were able to generate a *long* key as compared to the conventional cryptographic techniques from the estimated channel phase, while in [10], they extend their system to the use of relay nodes. Another channel based approach that generates a secondary random process from the estimated channel gain or phase is presented in [11]. The secret key generated from the secondary random process provided a drastic improvement in the achieved bit mismatch rate (BMR), which is the ratio of the key bits that do not match at the two nodes.

One main advantage of exploiting channel estimates to generate the secret key is its high key generation rate.

[1] From a practical perspective this would make the presence of Eve detectable by either Alice or Bob.

[2] The reader is referred to the references within [1] for further information on these types of attacks, called *active attacks*.

However, a main drawback of exploiting the channel reciprocity to generate secret keys is that the additive white Gaussian noise (AWGN) at both receivers affects the reciprocity of the channel measurements. Also, both nodes must collect the measurement simultaneously [12].

2.2. Received signal strength indicator

Other reciprocal (common) parameters such as received signal strength (RSS), which is a measure of the received signal's power, can be used as a common source of randomness to generate the secret key [4]. Their results showed that it would require a signal to noise ratio (SNR) of at least 20 dB to generate a secret with appropriate agreement. A practical implementation of RSS based secret key generation presented in [13] showed that it would require a highly mobile scenario to generate a secret key with acceptable entropy, i.e., key randomness.

RSS is a very common metric that requires a simple circuitry to be implemented. Nevertheless, its practical utilization as a common source of randomness is limited because its key bit generation rate is very low, particularly, for mobile scenarios [14].

2.3. Distance

A recent physical layer security technique that is based on the distance reciprocity to generate secret key bits is presented in [5]. Secret key generation based on distance is best suited for mobile scenario. The authors in [5] studied the theoretical achievable secret key bit rate in terms of the observation noise variance at the legitimate nodes and the eavesdropper. They also tested their algorithm using on-shelf radios. Most of the currently deployed localization techniques exploit the RSS to estimate the distance between the two communicating nodes [15]. Estimating the distance based on RSS requires an accurate modelling of the channel between the nodes. Moreover, it has a low estimation accuracy. This implies that the secret key generated based on distance will have a high BMR. There are other techniques to perform localization which are based on the time of arrival (TOA). Although localization based on TOA has a higher accuracy than RSS based, it requires a clock synchronization between the two nodes. Nevertheless, their estimation error is high at low SNR (<0 dB).

Secret key generation based on distance is developed for mobile scenarios where either of the two nodes are moving and therefore the distance between the two legitimate nodes changes. On the other hand, secret key generated based on the distance between the two communicating nodes is susceptible to be recovered by an eavesdropper that is equipped with angle of arrival (AoA) estimation capabilities. In this case, the eavesdropper estimates the AoA for both the signal received from the two nodes as well as the distances between itself and the two nodes. The eavesdropper then easily estimates the distance between the two nodes. Once the distance between the nodes is estimated, the secret key is recovered by the eavesdropper.

2.4. Angle of arrival

The authors in [16] presented a secret key generation algorithm that is based on the received signal's AoA. The authors compared the performance of generating a secret key based on AoA using different AoA estimation algorithms. They studied the root mean square error (RMSE) of AoA estimation using different techniques and they used that as an input to their simulation. The AoA, when measured from a common reference, will be equivalent at the two nodes. The authors studied the performance of their algorithm when changing the number of quantization bits and number of encoding bits. They also exploited both azimuth and elevation angles.

One main advantage of using the AoA as a common source of randomness is their high estimation accuracy at low SNR levels. On the other hand, to do so, the receiver must be equipped with AoA estimation capabilities such as smart antenna systems as well as employing a signal processing technique such as multiple signal classification (MUSIC), which increases both hardware and computational complexities.

3. Secret key generation steps

The steps to generate the secret key from the physical layer characteristics are based on whether a single or multiple common sources of randomness are used to extract the key. It is inherited that both Alice and Bob have already agreed on the common source(s), which will be used to generate the key. The vast majority of the current research work exploits only a single common source of randomness, i.e., 1-D. We explore the possibility of exploiting multiple common sources of randomness and show how the technique used to extract the secret key will differ. We first present the steps needed to extract the key exploiting 1-D common source of randomness followed by the addition needed to extract the key in case of multiple common sources of randomness.

3.1. Exploiting 1-D common source of randomness to extract the key

A block diagram of the steps needed to extract the key from a single common source of randomness is shown in Fig. 2. The block diagram includes all the necessary steps involved in the process of secret key generation. The two legitimate nodes start by an initializing phase followed by estimating the underline common randomness. Quantization, encoding, information reconciliation and privacy amplification steps are followed to convert the common randomness into a bit stream. The output of the block diagram is the secret key, which both legitimate nodes use to encrypt the transmitted data. The detailed steps are:

3.1.1. Initialization

This step is also known as *beacon exchange*. Both Alice and Bob start to exchange signal from which the physical layer characteristic will be estimated. Multiple beacon exchange might be needed based on the required length and rate of the key.

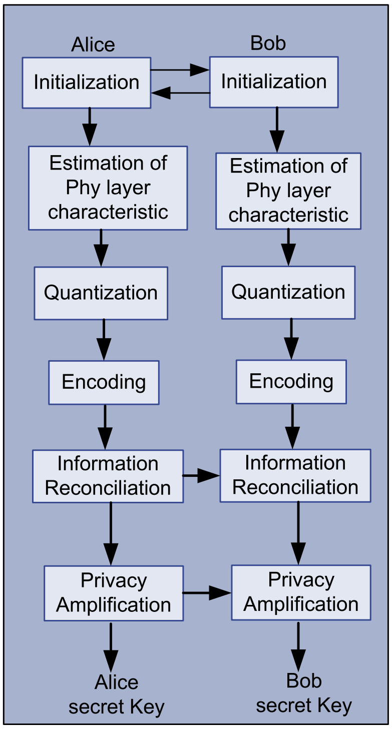


Fig. 2. Secret key generation steps in case of 1-D common source of randomness.

3.1.2. *Common source of randomness estimation*

Based on the received signal from the other legitimate node, both Alice and Bob estimate the physical layer characteristic. The estimation technique applied at either Alice or Bob does not necessarily be the same. For example, when exploiting the AoA to generate the secret key, Alice can use the popular MUSIC technique to estimate the angle, which is computationally expensive, while Bob can use the conventional beam switching technique, which has much lower hardware and computational complexities.

3.1.3. *Quantization*

Now that we have the common sources of randomness estimated at both Alice and Bob, the third step is to convert them into a bit stream suitable for the secret key generation. The conventional secret key length is between 128 and 512 bits [6]. The most popular technique for quantization is the uniform quantization. When using n_{quan} bits as the number of quantization bits, there will exist $2^{n_{quan}}$ levels to quantize the common sources of randomness. The quantized decimal values are then converted into bits. Moreover, the authors in [17–19] use a multi bit quantization technique, which uses multiple thresholds and which differs based on the selection of the threshold, to reduce the quantization error.

3.1.4. *Encoding*

Although uniform quantization is easy to implement, increasing the quantization bit number, dramatically degrades the performance of the algorithm since the bit mismatch rate between the two communicating nodes increases. In [20], an encoding algorithm is proposed to tackle this problem where each uniformly quantized value is encoded with multiple values, n_{encod} bits.

3.1.5. *Information reconciliation*

The generated bit streams at Alice and Bob will have some discrepancy, particularly at very low SNR levels. This is due to several reasons such as interference, noise and hardware limitations. A reconciliation protocol such as the one presented in [21] will be used to minimize the discrepancy. Both Alice and Bob first permute their bit streams in the same way. Then they divide the permuted bit stream into small blocks. Alice then sends permutations and parities of each block to Bob. Bob then compares the received parity information with the ones he already processed. In case of a parity mismatch, Bob changes his bits in this block to match the received ones. Another approach for information reconciliation is presented in [22], where the reconciliation step is treated as a source coding with side information problem. In this case, Alice compresses her collected common source of randomness data and Bob decodes them with the aid of his correlated collected data. Their reconciliation procedure can accomplish security rates comparable to the theoretical limits. Their method relies on multilevel coding and optimized low-density parity-check (LDPC) codes, where Alice applies a labelling function on its generated bit stream then produces supplementary information for Bob by calculating syndromes of the bit stream.

3.1.6. *Privacy amplification*

Although information reconciliation protocol leaks minimum information, the eavesdropper can still use this leaked information to guess the rest of the secret key. Privacy amplification solves this issue by reducing the length of the outputted bit stream. The generated bit stream is shorter in length but higher in entropy. To do so, both Alice and Bob apply a universal hash function selected randomly from a set of hash functions known by both Alice and Bob. Alice sends the number of the selected hash function to Bob so that Bob can use the same hash function.

3.2. *Exploiting multiple common sources of randomness to extract the key*

In some cases, it is possible to collect multiple common sources of randomness simultaneously such as channel gain and phase, channel real and imaginary coefficients [23], AoA azimuth and elevation angles [16], linear combination of channel estimates in multiple antenna scenario [24], RSS and distance, if distance estimation is based on RSS and channel gain and distance [25]. In other cases, the nodes might choose to collect multiple common sources of randomness not simultaneously such as channel gain and distance.

If multiple common sources of randomness were estimated and the nodes intend to exploit them to generate the secret key, the steps to generate the secret key are the same as in Fig. 2 with a block added either at the raw data level after *Estimation of Phy Layer Characteristic* block or at the bit level after the *Encoding* block. The responsibility of this block is to combine the multiple common sources of randomness. We shall call the step of combining the multiple common sources of randomness as the Fusion Operation.

4. Metrics to evaluate the generated secret key

We present the most commonly used metrics to evaluate the generated secret key, which can be categorized into two main categories: information theoretic metrics and statistical metrics.

4.1. Information theoretic metrics

We present three important information theoretic metrics, which are the secret key rate, the secret key capacity and the outage secret key capacity.

4.1.1. Secret key rate

The concept of secret key rate, R, was first presented in the pioneering work of Maurer in 1993 [26]. He derived the upper and lower bounds on the secret key rate considering that the two legitimate nodes, Alice and Bob, have unlimited access to a public channel, which Eve can listen to. Both Alice and Bob observe n independent and identically distributed random variable X and Y, respectively. X and Y are denoted by $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_n)$. At any instant of time i, the corresponding observations at Alice and Bob X_i and Y_i are highly dependent. These observations are their estimates of the common source of randomness. On the other hand, Eve observes a sequence of observation denoted by Z. The upper bound on the generated secret key as defined by Maurer is given by:

$$S(X; Y \parallel Z) \le \min\left[I(X;Y), I(X;Y|Z)\right] \tag{1}$$

where $I(X;Y)$ is the mutual information between X and Y and $I(X;Y|Z)$ is the mutual information between X and Y given Z. The lower bound is given by

$$S(X; Y \parallel Z) \ge \max\left[I(Y;X) - I(Z;X), I(X;Y) - I(Z;Y)\right]. \tag{2}$$

4.1.2. Secret key capacity

The supremum of the secret key rate is considered the secret key capacity C_s. Although, secret key capacity in general is still an open problem, Maurer defined it as:

$$\begin{aligned} C_s &= \max_{P_X} S(X; Y \parallel Z) \\ &\le \min\left[\max_{P_X} I(X;Y), \max_{P_X} I(X;Y|Z)\right] \end{aligned} \tag{3}$$

where P_X is the probability density function of X.

4.1.3. Outage secret key capacity

The outage secret key capacity can be given by [27]:

$$\mathcal{O}(R,\delta) = \mathcal{O}_{eq}(R,\delta) \cup \mathcal{O}_{ch}(R,\delta), \tag{4}$$

where δ is the parameter that represents the error event and $\mathcal{O}_{eq}(R,\delta)$ and $\mathcal{O}_{ch}(R,\delta)$ are the equivocation outage and the channel outage, respectively. In the context of exploiting the channel gain as a common source of randomness, the equivocation outage, which happens when the equivocation rate is less than $R - \delta$, is defined as:

$$\mathcal{O}_{eq}(R,\delta) = \left\{\frac{1}{n} H(W|Z,h) < R - \delta\right\}, \tag{5}$$

where $H(\cdot)$ denotes the entropy rate, W is the message, Z is the received signal by the eavesdropper and h is the available channel state information at the eavesdropper. The channel outage is given by:

$$\mathcal{O}_{ch}(R,\delta) = \left\{\frac{1}{n} I(T;Y) < R\right\}, \tag{6}$$

where T is the transmitted signal from Alice to Bob and Y in this context is the received signal by Bob.

4.2. Statistical metrics

The statistical tests applied on the secret key generated based on a physical layer characteristic are borrowed from the conventional cryptography test. As stated in [28] “Each statistical test determines whether the sequence possesses a certain attribute that a truly random sequence would be likely to exhibit; the conclusion of each test is not definite, but rather probabilistic”. The National Institute of Standards and Technology (NIST) (US Department of Commerce) [29] provides tools (Public key interoperability test suite certification path validation [30]) to evaluate the statistical metrics of the generated secret key. The tools are developed to evaluate the performance of conventional cryptographic techniques, however the generated key through a physical layer characteristic can be tested using the provided tools by NIST. There are five basic statistical tests presented in [28]. We add a more recent test applied on the generated secret key, which is the bit mismatch rate between the key generated at Alice and Bob. For a generated secret key s of length N bits, the six tests are:

4.2.1. Frequency test

The objective of this test is to determine if the number of 1’s and 0’s are approximately the same, as predicted for a random binary sequence.

4.2.2. Serial test

The objective of this test is to determine if the number of occurrences of the two bit subsequences 00, 01, 10, and 11 are approximately the same, as predicted for a random binary sequence.

4.2.3. Poker test

To apply the poker test, the generated key s is divided into k non-overlapping subsequences of length m. The objective of this test is to determine if the number of occurrences of each of the subsequences of length m is approximately the same, as predicted for a random binary sequence. If the length of the subsequence $m = 1$, the poker test reduces to the frequency test.

Table 1
A qualitative comparison between exploiting current state-of-the-art common sources of randomness.

	Channel estimates	RSS	Distance	AoA
Hardware complexity	Low/medium	Low	low/medium	High [16]
Computat. complexity	Low/medium	Low	Low	High [16]
Inherited 2-D sources	Yes	No	Yes	Yes
Mobility required	No	No	Yes	Yes
Key rate	High (10–35 bit per observation) [31]	Dependson mobility (ex: 2–4 bit per observation [18])	Dependson mobility (ex: 0.1 –0.8 bit per observation [5])	Depends on mobility [16]
Performance at low SNR levels	Low [16]	Low [16]	Medium [16]	High [16]

4.2.4. *Runs test*

Each run is represented as subsequence of the generated key s consisting of consecutive 0's or consecutive 1's. The subsequence of consecutive 0's is referred to as *gap*, while the subsequence of 1's is referred to as *block*. The objective of this test is to check if the number of runs of different lengths is as predicted for a random binary sequence. The expected number of runs (either gaps or blocks) of length j in the generated key s of length N is $e_j = (N - i + 3)2^j$.

4.2.5. *Autocorrelation test*

The objective of this test is to examine the correlation between the generated secret key s and a shifted version of itself.

4.2.6. *Bit Mismatch Rate*

The objective of this test is to estimate the bit mismatch between the two sequences generated at Alice and Bob. The BMR should be less than a threshold to meet reliability criteria.

5. Discussion

5.1. *Current state-of-the-art*

A main drawback in almost all of the existing physical layer security techniques, whether it is based on channel gain, RSS or distance, is their poor performance at low signal to noise ratio (SNR). Estimating the channel gain at low SNR levels will result in a high error due to the effect of the AWGN. Similarly, for RSS case and consequently distance estimation based on the RSS. One main advantage of exploiting the AoA is their high estimation accuracy at very low SNR levels resulting in a very low BMR compared to other techniques at these low levels. This comes at the cost of high hardware and computational complexities. A qualitative comparison between exploiting different common sources of randomness is presented in Table 1.

5.2. *BMR simulation results*

We test the BMR exploiting the most common physical layer characteristics which are channel gain, channel phase, RSS, azimuth angle and elevation angle. In addition to that we combine the channel gain and phase and the azimuth and elevation angles. The simulation settings for Figs. 3 and 4 are:

- We generate beacon signals at both Alice and Bob.
- The beacon signals are passed through a Rician fading channel before adding AWGN. We chose a Rician channel since its multipath comprises a line of sight, which is required for AoA estimation such that the environment secret key generation based on AoA is the same for the channel.
- We estimate the RSS at both Alice and BoB.
- We estimate the channel gain and phase of the Rician channel.
- We generate random azimuth and elevation angles RMSE of up to two degree up to SNR $=$ 15 dB. In fact, this can be considered a high RMSE since most of the AoA estimation techniques have a lower RMSE at this SNR range. We chose to do so to accommodate the worst case AoA estimation techniques.
- For a fair comparison between the different common sources of randomness, we first scale the sequence of information collected to the same scaling level such that all common sources of randomness used below, fluctuate within the same levels.
- We apply the steps in Fig. 2 to the encoding for RSS, channel gain only, channel phase only, azimuth angle only and elevation angle only. We add the combining step when exploiting channel gain and phase and azimuth and elevation angles as 2-D common sources of randomness.
- After generating the secret key at Alice and Bob, the BMR is calculated between the two keys.
- The simulation is run for 10000 iteration to estimate the average BMR.
- We repeat the steps above to cover the SNR range of interest.
- A threshold is added at BMR $= 0.15$ depicting a reliability constraint on the BMR.
- The legends notations in Figs. 3 and 4 are presented in Table 2.

The fusion operation : The objective of the fusion operation is to combine the two common sources of randomness so as to reduce the BMR after the quantization step, which leads to a longer key. In addition, combining multiple common sources of randomness increases the secret key rate.

- We chose to combine the two common sources of randomness in the bit stream level rather than as a raw data.

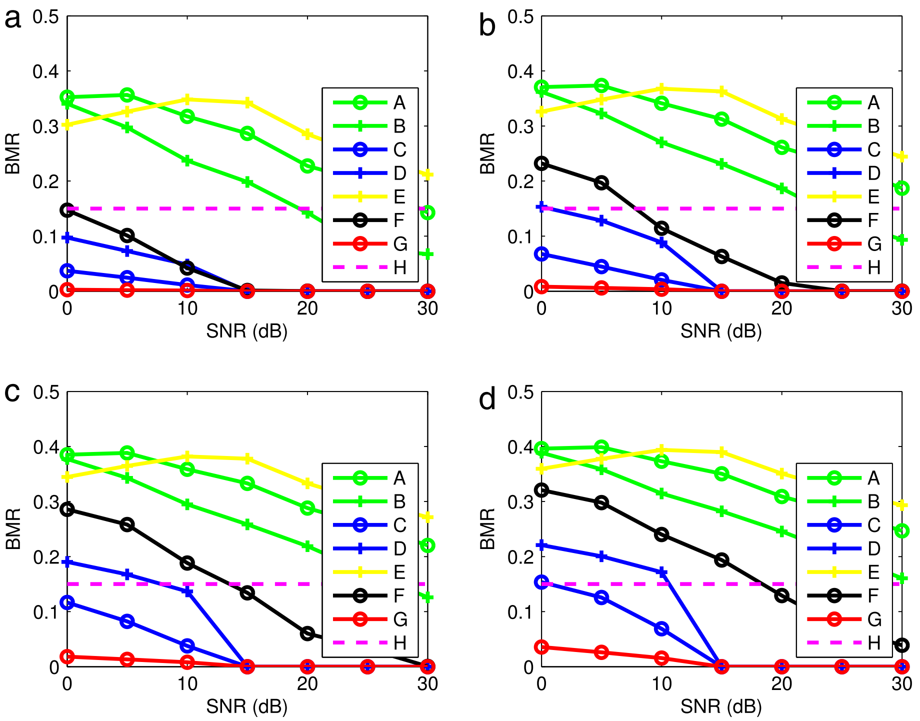


Fig. 3. BMR vs. SNR for different number of quantization bits: (a) 5 bits, (b) 6 bits, (c) 7 bits and (d) 8 bits.

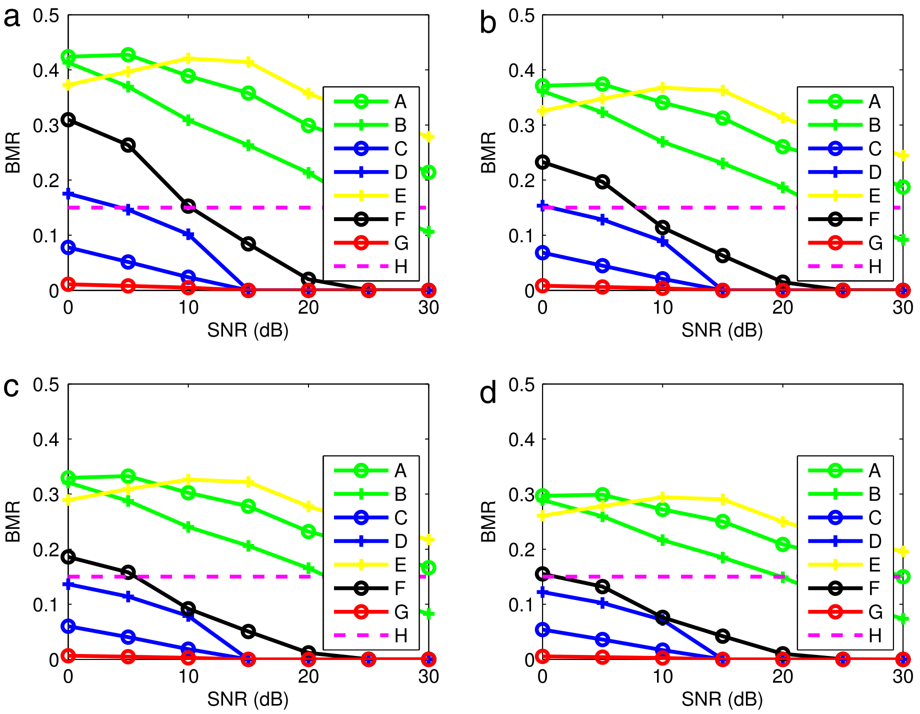


Fig. 4. BMR vs. SNR for different number of encoding bits: (a) 1 bits, (b) 2 bits, (c) 3 bits and (d) 4 bits.

Table 2
Legend notations for Figs. 3 and 4.

A	B	C	D	E	F	G	H
Chan. gain	Chan. phase	Az. angle.	Elev. angle	RSS	Comb. gain. & ph	Comb. Az. & Elev	Thresh.

- To combine the two bit streams, any logical operation such as AND, OR or concatenation can be applied on the two bit streams to generate a single bit stream containing both channel gain and phase and azimuth and elevation angles.
- We choose to use concatenation operation with the two bit streams as the inputs to generate the single bit stream.
- To improve the BMR, before we concatenate, we drop the least significant ($n_{quan} - n_{combn}$) bits from each single bit stream, where n_{comb} is the number of bits selected from each bit stream.

It is worth noting that we chose a simple bit operation to be applied on the bit streams for the sake of simplification. One can apply a more complicated operation at the bit streams such as bit masking or combinations of series and parallel logical gates.

Fig. 3 shows the BMR for different n_{quan} using $n_{encod} = 2$ and $n_{comb} = 5$. Fig. 4 shows the BMR for different n_{encod} using $n_{quan} = 6$ and $n_{comb} = 5$. We simulate the secret key generation for the different common sources of randomness up to the encoding step. It can be inferred from the two figures that RSS based secret key generation is achieving the worst results. As expected, as the number of quantization bits increases, the BMR increases. Also, as the number of encoding bits increases, the BMR decreases. In addition to that a high SNR is required to achieve an adequate BMR for the channel gain, channel phase and RSS. The azimuth and elevation angles on the other hand can operate with very low BMR at low SNR levels. It also can be inferred that the information reconciliation step will be more laborious in the case of channel gain only, channel phase only and RSS than azimuth and elevation angles case.

In addition to that, a main advantage of exploiting multiple common sources of randomness is that it can drastically improve the BMR even when using a simple bit operation such as concatenation after dropping the LSBs. As can be seen, when combining both channel gain and phase, the BMR improved significantly. Another main advantage of exploiting multiple common sources of randomness is that the key length will increase substantially. More simulation results that address some of the above metrics can be found in [32].

5.3. Roadmap to the future

Hybridization for key generation

As mentioned earlier, nodes can always benefit from estimating multiple common sources of randomness simultaneously. As shown earlier in the case of using angle arrival as a common source of randomness, where two independent angles were combined to generate the secret key using a simple concatenation operation, the BMR improved drastically. The problem of combining multiple common sources of randomness whether as raw data or bit streams remains an open research direction. Different hybridization (i.e., combining) functions can be applied on the multiple common sources of randomness with the objective of minimizing the BMR and maximizing the key entropy. In addition to that exploiting multiple common sources of randomness adds an extra degree of freedom to the legitimate nodes since the function, which they will apply on the common sources of randomness will be hidden from the eavesdropper.

Towards convergence of physical layer and cryptographic secrecy

Till date, the two worlds of physical layer secrecy and cryptographic secrecy speak two different languages. While the former can only measure a non-vanishing secrecy capacity under the assumptions of infinitely long keys without any key reuse and assuming an infinite computation capabilities for the eavesdropper, the latter measures secrecy under finite computational capabilities of the eavesdropper, finite key lengths and mandatory key reuse. It would be highly desirable to find a way to converge the two worlds in order to allow for practical comparisons between conventional cryptographic methods and relatively recent physical layer secrecy based methods. There is a potential to move the information theoretic measures of the physical layer based methods towards more practical measures using some approximate representations of secrecy capacity under certain allowable probabilities of key breaking by the eavesdropper providing promising results towards arriving at common secrecy measures that can be used by the two worlds.

6. Conclusion

In this paper, we presented a survey on the most recent physical layer characteristics used to generate the secret key. We presented the steps needed to extract the secret key from the estimated common source of randomness. We then presented the metrics used to evaluate the strength of the key. We studied the performance of exploiting different common sources of randomness through BMR simulation. We then presented a qualitative comparison between them. In addition to that, we discussed the open research problem within the subject.

Acknowledgements

This research was made possible by NPRP 5-559-2-227 grant from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] A. Mukherjee, S. Fakoorian, J. Huang, A. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey, IEEE Commun. Surv. Tutor. 16 (3) (2014) 1550–1573. http://dx.doi.org/10.1109/SURV.2014.012314.00178.

[2] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387. http://dx.doi.org/10.1002/j.1538-7305.1975.tb02040.x.

[3] R. Wilson, D. Tse, R. Scholtz, Channel identification: Secret sharing using reciprocity in ultrawideband channels, IEEE Trans. Inf. Forensics Secur. 2 (3) (2007) 364–375. http://dx.doi.org/10.1109/TIFS.2007.902666.

[4] A. Kitaura, H. Iwai, H. Sasaoka, A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio, in: The 9th International Conference on Advanced Communication Technology, Vol. 3, 2007, pp. 1763–1767. http://dx.doi.org/10.1109/ICACT.2007.358712.

[5] O. Gungor, F. Chen, C. Koksal, Secret key generation via localization and mobility, IEEE Trans. Veh. Technol. PP (99) (2014) 1. http://dx.doi.org/10.1109/TVT.2014.2342714.

[6] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel, in: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, MobiCom '08, 2008, pp. 128–139.

[7] Z. Li, W. Xu, R. Miller, W. Trappe, Securing wireless systems via lower layer enforcements, in: Proceedings of the 5th ACM Workshop on Wireless Security, WiSe '06, 2006, pp. 33–42.

[8] A.A. Hassan, W.E. Stark, J.E. Hershey, S. Chennakeshu, Cryptographic key agreement for mobile radio, Digit. Signal Process. 6 (4) (1996) 207–212. http://dx.doi.org/10.1006/dspr.1996.0023. URL http://www.sciencedirect.com/science/article/pii/S1051200496900238.

[9] H. Koorapaty, A. Hassan, S. Chennakeshu, Secure information transmission for mobile radio, in: 1998 IEEE International Symposium on Information Theory, 1998. Proceedings, 1998, p. 381. http://dx.doi.org/10.1109/ISIT.1998.708986.

[10] Q. Wang, K. Xu, K. Ren, Cooperative secret key generation from phase estimation in narrowband fading channels, IEEE J. Sel. Areas Commun. 30 (9) (2012) 1666–1674. http://dx.doi.org/10.1109/JSAC.2012.121010.

[11] A. Badawy, T. Khattab, T.M. Elfouly, C.-F. Chiasserini, A. Mohamed, D. Trinchero, Channel secondary random process for robust secret key generation, in: IWCMC 2015 Security Symposium, IWCMC 2015 Security Symposium, Dubrovnik, Croatia, 2015.

[12] N. Patwari, J. Croft, S. Jana, S. Kasera, High-rate uncorrelated bit extraction for shared secret key generation from channel measurements, IEEE Trans. Mobile Comput. 9 (1) (2010) 17–30. http://dx.doi.org/10.1109/TMC.2009.88.

[13] S.N. Premnath, S. Jana, J. Croft, P.L. Gowda, M. Clark, S.K. Kasera, N. Patwari, S.V. Krishnamurthy, Secret key extraction from wireless signal strength in real environments, IEEE Trans. Mobile Comput. 12 (5) (2013) 917–930.

[14] K. Ren, H. Su, Q. Wang, Secret key generation exploiting channel characteristics in wireless communications, IEEE Wirel. Commun. 18 (4) (2011) 6–12. http://dx.doi.org/10.1109/MWC.2011.5999759.

[15] N. Patwari, A.O. Hero III, Using proximity and quantized rss for sensor localization in wireless networks, in: Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications, WSNA '03, 2003, pp. 20–29.

[16] A. Badawy, T. Khattab, T. Elfouly, D. Mohamed, A. Trinchero, C. Chiasserini, Secret key generation based on aoa estimation for low snr conditions, in: 2015 IEEE 81st Vehicular Technology Conference, VTC Spring, 2015, pp. 1–7.

[17] S. Jana, S.N. Premnath, M. Clark, S.K. Kasera, N. Patwari, S.V. Krishnamurthy, On the effectiveness of secret key extraction from wireless signal strength in real environments, in: Proceedings of the 15th Annual International Conference on Mobile Computing and Networking, MobiCom '09, 2009, pp. 321–332.

[18] H. Liu, J. Yang, Y. Wang, Y. Chen, Collaborative secret key extraction leveraging received signal strength in mobile wireless networks, in: 2012 Proceedings IEEE, INFOCOM, 2012, pp. 927–935. http://dx.doi.org/10.1109/INFCOM.2012.6195843.

[19] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, H. Sasaoka, Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels, IEEE Trans. Antennas Propag. 53 (11) (2005) 3776–3784. http://dx.doi.org/10.1109/TAP.2005.858853.

[20] J. Zhang, S. Kasera, N. Patwari, Mobility assisted secret key generation using wireless link signatures, in: 2010 Proceedings IEEE, INFOCOM, 2010, pp. 1–5. http://dx.doi.org/10.1109/INFCOM.2010.5462231.

[21] G. Brassard, L. Salvail, Secret-Key Reconciliation by Public Discussion, Springer-Verlag, 1994, pp. 410–423.

[22] M. Bloch, J. Barros, M. Rodrigues, S. McLaughlin, Wireless information-theoretic security, IEEE Trans. Inform. Theory 54 (6) (2008) 2515–2534. http://dx.doi.org/10.1109/TIT.2008.921908.

[23] Y. Liu, S. Draper, A. Sayeed, Exploiting channel diversity in secret key generation from multipath fading randomness, IEEE Trans. Inf. Forensics Secur. 7 (5) (2012) 1484–1497. http://dx.doi.org/10.1109/TIFS.2012.2206385.

[24] C.D.T. Thai, J. Lee, C. Cheng, T. Quek, Physical-layer secret key generation with untrusted relays, in: Globecom Workshops, GC Wkshps, 2014, 2014, pp. 1385–1390. http://dx.doi.org/10.1109/GLOCOMW.2014.7063627.

[25] A. Badawy, T. Khattab, T. Elfouly, A. Mohamed, D. Trinchero, Secret key generation based on channel and distance measurements, in: 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT, 2014, pp. 136–142. http://dx.doi.org/10.1109/ICUMT.2014.7002092.

[26] U. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inform. Theory 39 (3) (1993) 733–742. http://dx.doi.org/10.1109/18.256484.

[27] O. Gungor, J. Tan, C. Koksal, H. El-Gamal, N. Shroff, Secrecy outage capacity of fading channels, in: 2012 46th Annual Conference on Information Sciences and Systems, CISS, 2012, pp. 1–6. http://dx.doi.org/10.1109/CISS.2012.6310770.

[28] A.J. Menezes, S.A. Vanstone, P.C.V. Oorschot, Handbook of Applied Cryptography, fifth ed., CRC Press, Inc., Boca Raton, FL, USA, 2001.

[29] Nist: Computer security resource center. URL http://csrc.nist.gov.

[30] Nist — csrs: Public key interoperability test suite certification path validation. URL http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/PKITS.pdf.

[31] C. Ye, A. Reznik, G. Sternberg, Y. Shah, On the secrecy capabilities of itu channels, in: 2007 IEEE 66th Vehicular Technology Conference, 2007, VTC-2007 Fall, 2007, pp. 2030–2034. http://dx.doi.org/10.1109/VETECF.2007.426.

[32] A. Saad, A. Mohamed, T. Elfouly, T. Khattab, M. Guizani, Comparative simulation for physical layer key generation methods, in: 2015 International Wireless Communications and Mobile Computing Conference, IWCMC, 2015, pp. 120–125. http://dx.doi.org/10.1109/IWCMC.2015.7289068.

Ahmed Badawy received his bachelors in Electrical Engineering from the University of Nevada, Reno, USA in 2008 and his M.Sc from Montana State University, Bozeman, USA in 2010. He is currently pursuing his Ph.D. at the Department of Electronics and Telecommunications at Politecnico di Torino, Italy. His research interests include cognitive radios, physical layer security, smart antenna systems and hardware implementation of communication systems.

Tarek Elfouly received his DEA and Ph.D. from the University of Franche Comte in France, in 1996 and 2000 respectively. He has worked as an assistant professor at the university of Ain Shams Cairo Egypt before joining Qatar University. He is currently an assistant professor in the college of engineering at Qatar University. He has over 10 years of experience in computer network research. Dr. Elfouly published over 40 papers, more than half of them are related to wireless sensing and network security. Dr. Elfouly has many projects under development related to assistive technologies for people with disabilities. His projects won many national and regional awards. His research interests include network security and protocols, physical layer security and wireless sensor networks especially in the field of structural health monitoring and health applications.

Tamer Khattab received his Ph.D. in Electrical and Computer Engineering from the University of British Columbia (UBC), Vancouver, BC, Canada in 2007, M.Sc. in Electronics and Communications Engineering and B.Sc. in Electronics and Communications Engineering from Cairo University, Giza, Egypt. Dr. Khattab has been an assistant professor of Electrical Engineering at Qatar University (QU) since 2007. He is also a senior member of the technical staff at Qatar Mobility Innovation Center (QMIC) an R&D center owned by QU and funded by Qatar Science and Technology Park (QSTP). Between 2006 and 2007 he was a postdoctoral fellow at the University of British Columbia working on prototyping advanced Gigabit/sec wireless LAN baseband transceivers. During 2000-2003 Dr. Khattab joined Alcatel Canada's Network and Service Management R&D in Vancouver, BC, Canada as a member of the technical staff working on development of core components for Alcatel 5620 network and service manager. Between 1994 and 1999 he was with IBM wtc. Egypt as a software development team lead working on development of several client-server corporate tools for IBM labs. Dr. Khattab's research interests cover physical layer transmission techniques in optical and wireless networks, information theoretic aspects of communication systems and MAC layer protocol design and analysis.

Amr Mohamed received his Ph.D. and M.S. in electrical and computer engineering from the University of British Columbia, Vancouver, Canada, in 2001, and 2006 respectively. He has worked as an advisory IT specialist in IBM Innovation Centre in Vancouver from 1998 to 2007, taking a leadership role in systems development for vertical industries. He is currently an associate professor in the college of engineering at Qatar University and the director of the Cisco Regional Academy. He has over 20 years of experience in wireless networking research and industrial systems development. He holds 3 awards from IBM Canada for his achievements and leadership, and 3 best paper awards. His research interests include networking and MAC layer techniques mainly in wireless networks. Dr. Mohamed has authored or co-authored over 80 refereed journal and conference papers and one textbook.

Mohsen Guizani (FELLOW OF IEEE) received the B.S. (with distinction) and M.S. degrees in electrical engineering and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor at the Department of Computer Science and Engineering, Qatar University (QU), Doha, Qatar. Previously, he served as the Associate Vice President of Graduate Studies at QU in 2011–2014; the Chair of the Department of Computer Science, Western Michigan University, in 2002–2006; and the Chair of the Department of Computer Science, University of West Florida, in 1999-2002. He also served in academic positions at the University of Missouri-Kansas City, University of Colorado-Boulder, Syracuse University, and Kuwait University. His research interests include wireless communications and mobile computing, computer networks, cloud computing, cyber security, and smart grid.

Dr. Guizani is a Senior Member of ACM and a member of the IEEE Communications Society, IEEE Computer Society, and ASEE. He currently serves on the Editorial Boards of several international technical journals and the Founder and Editor-in-Chief of Wiley's Wireless Communications and Mobile Computing (http://www.interscience.wiley.com/jpages/1530-8669/). He is the author of nine books and more than 400 publications in refereed journals and conferences (with an h-index = 30 according to Google Scholar). He guest edited a number of special issues in IEEE journals and magazines. He also served as a Member, Chair, and General Chair of a number of conferences. He was the Chair of the IEEE Communications Society Wireless Technical Committee (WTC 2009–2010) and the Chair of the Transmission, Access and Optical Systems (TAOS 2007–2009). He served as the IEEE Computer Society Distinguished Speaker from 2003 to 2005. He received the Best Research Award from two institutions.