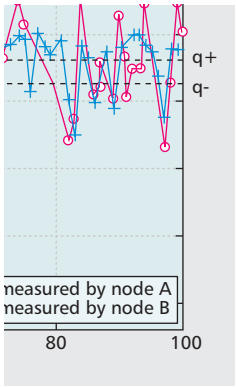
ACCEPTED FROM OPEN CALL

SECRET KEY GENERATION EXPLOITING CHANNEL CHARACTERISTICS IN WIRELESS COMMUNICATIONS

KUI REN, HAI SU, AND QIAN WANG, ILLINOIS INSTITUTE OF TECHNOLOGY



The authors provide an overview of the existing PHY-based key generation schemes exploiting the randomness of the wireless channels.

ABSTRACT

Due to the broadcast nature of wireless channels, wireless communication is vulnerable to eavesdropping, message modification, and node impersonation. Securing the wireless communication requires the shared secret keys between the communicating entities. Traditional security schemes rely on public key infrastructures and cryptographic algorithms to manage secret keys. Recently, many physical-layer-based methods have been proposed as alternative solutions for key generation in wireless networks. These methods exploit the inherent randomness of the wireless fading channel to generate secret keys while providing information-theoretical security without intensive cryptographic computations. This article provides an overview of the existing PHY-based key generation schemes exploiting the randomness of the wireless channels. Specifically, we first introduce the fundamental and general framework of the PHY-based key generation schemes and then categorize them into two classes: received-signal-strength-based and channel-phase-based protocols. Finally, we present a performance comparison of them in terms of key disagreement probability, key generation rate, key bit randomness, scalability, and implementation issues.

INTRODUCTION

Due to the inherently shared nature of the wireless medium, the security of the wireless network is threatened by eavesdropping, message modifying, and node impersonating. To protect the confidentiality, integrity, and authenticity of the communication, secret keys must be established for securing wireless networks. Recently, a family of key generation methods exploiting physical layer (PHY) information and techniques is caught in hot discussion as alternative keying protocols in wireless networks. Compared to the traditional Diffie-Hellman key agreement protocol that relies on computational hardness of problems, these PHY-based methods do not assume a computationally bounded adversary (i.e., they can achieve information-theoretical security). These methods are constructed on the properties of the wireless channel:

- Channel randomness: The channel fading is random along time due to multipath propagation.
- Independent channel variation over space: A third party who lies one-half wavelength away from the legitimate transceivers experiences fading that is uncorrelated to that between the legitimate parties.
- Channel reciprocity: The two transceivers that lie on the ends of the same wireless link experience multipath fading that is theoretically identical.

In these PHY-based key generation methods, by alternatively sending probe signals and estimating the common random channel state, the legitimate parties can convert their channel estimates into the same bit strings. The bit discrepancies are corrected using key reconciliation and privacy amplification techniques [1, 2]. The performance of these schemes is usually measured in terms of:

- Key agreement probability, which characterizes the robustness of the key generation schemes
- Secret key generation rate, which measures the efficiency of the schemes
- Key bit randomness, which measures the randomness of the generated keys

In this article, we further extend the performance analysis by discussing the scalability and implementation complexity issues.

Theoretic research on PHY-based key generation can be traced back to the original information-theoretical formulation of secure communication due to [3]. Building on information theory, [4, 5] characterized the fundamental bounds, and showed the feasibility and gains of generating keys using external random source-channel impulse response. However, they only aimed at deriving theoretical limits and did not provide practical key generation algorithms in wireless networks. Using multipath channels as the source of common randomness, recent research has focused on measuring a popular statistic of wireless channel, received signal strength (RSS), for extracting shared secret bits between node pairs [6–8]. It has been demonstrated that these RSS-based methods are feasible in existing platforms. However, they also suffer from some problems such as low key bit

1536-1284/11/$25.00 © 2011 IEEE

generation rate and scalability issues. To address these problems, a key generation scheme based on channel phase estimation was proposed in [9], which allowed effective accumulation of channel phases across multiple nodes. In this article, we provide an overview of the PHY-based key generation schemes and discuss the recent progress in this area. The goal of this article is to aid future designs of more secure and robust key generation schemes exploiting channel randomness.

Principles and Preliminaries

System Model and Threat Model

The PHY-based key generation schemes discussed in this article are all based on the channel-type model shown in Fig. 1, where Alice and Bob are legitimate parties that want to establish a pairwise key K_{AB}, and Eve is a passive adversary that aims to derive the K_{AB} by eavesdropping. All network nodes are assumed to be half-duplex in the sense that they cannot transmit and receive signals at the same frequency simultaneously. If the channel between Alice and Bob is reciprocal, by transmitting signals in forward and backward directions, the legitimate parties can develop correlated information for key bit extraction. The passive adversary Eve is assumed to be a computationally unbounded eavesdropper, and it can eavesdrop on all the communications between Alice and Bob.

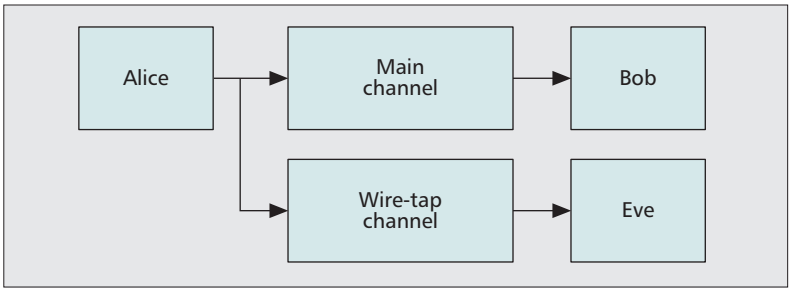


Figure 1. *System model for key generation in wireless communication.*

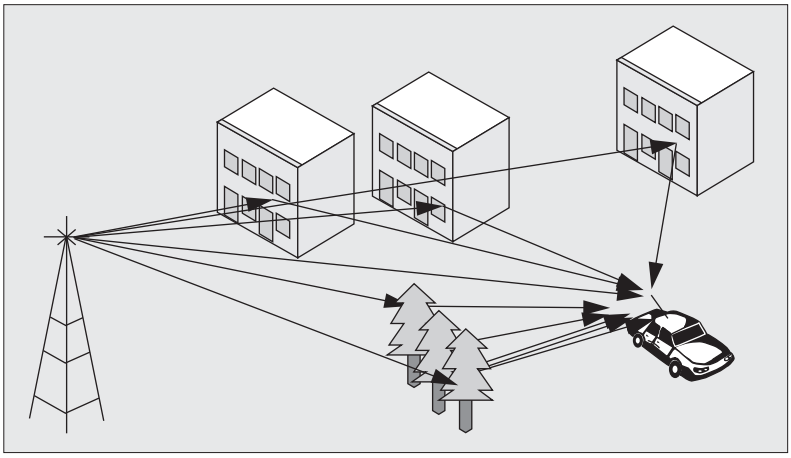


Figure 2. *An example of a multipath channel.*

Characteristics of a Multipath Fading Channel

The characteristics of a multipath fading channel have been widely studied in the wireless communication literature. For completeness, here we introduce its features that are essential to PHY-based secret key generation. When the magnetic waveform propagates through a wireless channel, due to the reflection, diffraction, and scattering caused by the objects between and around the transceivers, the signal arrives the receiver in multiple paths; see an example in Fig. 2. The received signal is a summation of signals from multiple paths with different delays. This summation can be either constructive or destructive, which depends on the relative propagation delays of signals. Furthermore, relative movement between the environment and the mobile terminals can change the paths randomly, which leads to random fluctuation in the phase and amplitude of the received signal. This random fluctuation gives birth to the following three properties that serve as the basis for key generation using characteristics of fading channels [8].

Temporal Variation — Due to the movements of the entities in the environment as well as the communicating parties themselves, the received signal experiences different fadings along time. Theoretically, the fading at two time points are independent if the interval between the two time points is larger than the channel *coherence time*. In wireless communications, coherence time is a statistical measure of the time duration over which the channel impulse response is essentially invariant, and quantifies the similarity of the channel response at different times.

Spatial Variation — In a multipath environment, receivers at different locations receive signals that experience different and independent fadings from the same transmitter. According to communication theory [10], an entity that is at least $\lambda/2$ (λ is the wavelength) away from the network nodes experiences fadings statistically independent of the fadings between the communicating nodes.

Reciprocity — The signals transmitted between a transmitter and receiver pair experience the same fading in the coherence time. This is because the propagation paths of the forward link and backward link are theoretically identical during the coherence time; see an example of channel reciprocity in Fig. 3. It is obvious that while the temporal and spatial variations can be exploited to meet the security goals, the reciprocity property can be exploited for key generation.

Key Generation Protocols

Based on the above discussions, we can see that PHY-based key generation protocols can exploit randomness and reciprocity of the wireless channel for key bit extraction. The common randomness is either extracted from the amplitude or phase of the received signals. Generally, a key generation scheme consists of three steps:

- Channel probing
- Measurement quantization
- Error correction

In the following, we discuss two classes of PHY-based key generation protocols: key bit

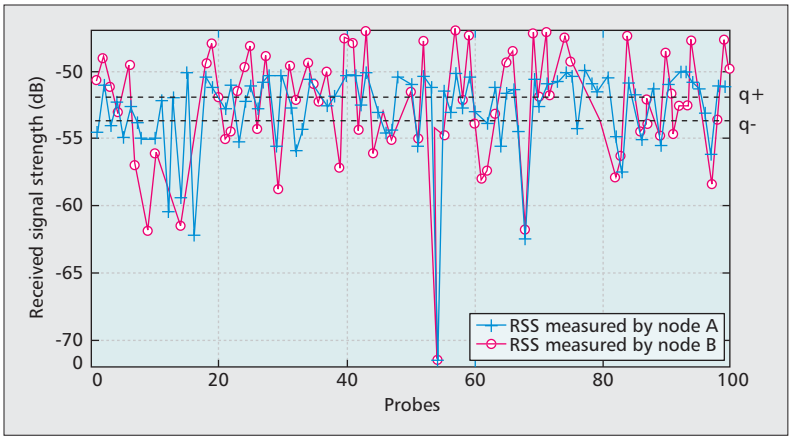


Figure 3. *An example of channel reciprocity based on received signal strength (RSS).*

extraction from RSS and key bit extraction from received signal phase.

Secret Key Extraction from Received Signal Strength

Received signal strength is a measurement of the power present in the received radio signal. Recently, practical RSS-based key generation schemes have been extensively studied [6–8]. However, the key bit generation rate supported by these approaches is very low. This significantly limits their practical usage given the intermittent connectivity in mobile environments. To address the problem, several enhanced schemes are proposed in [11, 12] to increase the key bit generation rate. In the rest of this section, we first introduce basic RSS-based key generation schemes and then present their enhanced versions.

Basic Schemes Using RSS — The basic schemes mainly consist of the following three steps:

Step 1: Channel probing. In the first timeslot, Alice transmits a known sequence S_A to Bob. Upon receiving the signal, Bob measures and records the RSS values of S_A. In the second time slot, Bob transmits a known sequence S_B to Alice. Upon receiving the signal, Alice measures and records the RSS values of S_B. The length of the time slot is usually set as half of the channel coherence time. If multiple rounds of channel probings are run during the same coherence time period, the randomness of the generated key bits is decreased.

Step 2: Measurement quantization. Both Alice and Bob convert their RSS measurements into random key bits using a quantizer,

$$Q(x) = \begin{cases} 1 & \text{if } x > q+ \\ 0 & \text{if } x < q-, \end{cases}$$

where x denotes the sample value, and $q+$ and $q-$ denote the upper and lower thresholds, respectively. The existing schemes use different rules to determine the thresholds and select samples. In [7], the thresholds are determined by calculating mean and standard deviation of the samples. To increase the probability of key agreement, m consecutive samples that are above $q+$ or below $q-$ are used to generate one bit. Due to the same reason, [6] only quantizes the matching deep fades of RSS measurements. In [8], Jana *et al.* proposed an adaptive secret bit generation (ASBG) scheme, where the measured RSS sequence is broken into smaller blocks and the thresholds are calculated for each block. It can remove the components that vary slowly and thus increase the entropy of the generated bit sequence. To increase the key bit generation rate, [8] adopts a multiple-bit extraction method, where a single RSS sample is converted into multiple bits using Gray codes. However, as multiple-bit extraction places a more strict constraint on the accuracy of RSS measurement and channel reciprocity, it may lead to an increased bit mismatch rate.

Step 3: Error correction. Alice and Bob reconcile the bit discrepancies between their generated keys. The bit discrepancies may be caused by noise, interference, hardware variations, and half-duplex probing signal transmission. Common practice is to use key reconciliation and privacy amplification techniques [2] for achieving key agreement.

Enhanced Variations Based on RSS — As discussed above, the key generation schemes based on RSS are subject to a trade-off between key bit generation rate and key bit mismatch rate. Several enhanced variations are investigated in [12, 13]. In [12], a multiple-antenna system is exploited to increase the key bit generation rate. The intuition behind this idea is that a multiple-antenna system provides more channel randomness for bit extraction. Since too many quantization levels may increase the key bit mismatch rate, they determine the quantization level by estimating the entropy of the measurements. In addition, they use a guard band between quantization bins to further guard the key agreement rate. The resulting key bit generation rate is increased by more than four times compared to that of single-antenna systems.

In [13], it is observed that nonsimultaneous channel measuring undermines the link reciprocity, while fractional interpolation can recover the reciprocity of the link. To do so, the nodes first sample the channel at a rate higher than the Nyquist frequency of the channel and use fractional interpolation to estimate what measurements would have been if they had been measured simultaneously. As a result, the measurements obtained by each node are highly correlated to each other due to the virtually high rate measurement. They further apply discrete Karhunen-Loeve transform (KLT) to remove the correlation among the measurements. Following the previous steps, multiple-bit adaptive quantization is applied. Different from the multiple-bit quantizer used in [8], Patwari *et al.* divide the RSS range into quantization bins according to the distribution of the measurements such that each bin contains the same amount of measurements. Doing so can potentially enhance the key bit randomness, and a higher key generation rate with sound randomness is achieved.

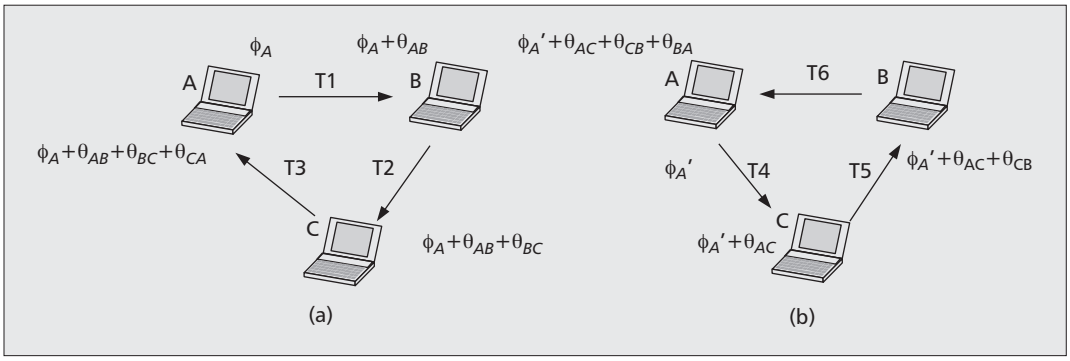


Figure 4. *Example of Group Key Generation: The beacon signal has the form* $s(t) = e^{jwt+\phi}$ *and the channel has the form* $h(t) = |h(t)|e^{j\theta}$. *In this figure, we only give the phase notations and eliminate the signal expressions for simplicity.* ϕ_A *and* ϕ'_A *denote the initial phases of the beacon signal in the clockwise and anticlockwise transmissions, respectively.* θ_{ij} *(*i, j θ {A, B, C}*) denotes the channel phase from node* i *to* j. *Due to channel reciprocity,* $\theta_{ij} = \theta_{ji}$.

Practical RSS-based key generation schemes have been extensively studied. However, the key bit generation rate supported by these approaches is very low. This significantly limits their practical usage given the intermittent connectivity in mobile environments.

Secret Key Extraction from Channel Phase

In this section, we discuss another class of PHY-based key generation schemes where the common randomness is extracted from the phase of received signal. Compared to RSS-based key generation schemes, channel-phase-based methods have three major advantages. First, the channel phase of the received signal has uniform distribution under narrowband fading channels [10]. Second, the existing signal processing technique allows for high resolution estimation of phase of the received signal, which implies that higher key generation rate is achievable. Third, the phase estimates can be accumulated across multiple nodes, which enables efficient group key generation. To the best of our knowledge, Hershey *et al.* proposed the first key generation scheme based on differential phase detection in [5]. In [14], Sayeed *et al.* proposed a channel-phase-based key generation scheme for OFDM systems. In [9], Wang *et al.* designed a suite of channel-phase-based key generation schemes that support both pairwise key and group key generation. The key steps of channel-phase-based key generation schemes are as follows.

Step 1: Channel probing. This step is similar to its counterpart in RSS based methods. The difference is that Alice and Bob estimate and record the phases of the common channel in the pairwise communication link. For the purpose of channel probing, the existing schemes adopt different probing signals. In [5], the probing signal consists of two single-tone sinusoid signals at frequency f_1 and f_2 with equal phase and power:

$$s(t) = \sqrt{\frac{2E}{T}}\cos(2\pi f_1 t + \phi) + \sqrt{\frac{2E}{T}}\cos(2\pi f_2 t + \phi).$$

The received signal can be written as

$$r(t) = \alpha_1(t)\sqrt{\frac{2E}{T}}\cos(2\pi f_1 t + \Theta_1(t)) + \alpha_2(t)\sqrt{\frac{2E}{T}}\cos(2\pi f_2 t + \Theta_2(t)),$$

where $\alpha_i(t)(i = 1, 2)$ denotes the attenuation factor due to fading, and $\Theta_i(t)(i = 1, 2)$ denotes the channel phase, which is uniformly distributed over $[0, 2\pi]$. The phase difference between the two single-tone sinusoid signals $\delta(\tau) = \Theta_1(t) - \Theta_2(t)$ is computed and recorded for quantization. In [14], Sayeed *et al.* proposed a key generation protocol for orthogonal frequency-division multiplexing (OFDM) systems that exploits the inherent channel phase randomness through channel estimation and quantization. In an OFDM system, a "single" channel utilizes multiple subcarriers on adjacent frequencies for transmission, each of which serves as one random source for bit extraction. Thus, it potentially increases the key bit generation rate. In [9], Wang *et al.* proposed a scalable and efficient key generation scheme exploiting channel phases. The basic idea behind their key generation scheme is to exploit the inherent channel randomness associated with distinct pairwise links; that is, the carriers transmitted back and forth along the clockwise and anticlockwise circuit experience the same phase variation over the same coherence time period. In Fig. 4, we illustrate their scheme using an example with three nodes, say *A*, *B* and *C*. For ease of exposition, we ignore the phase estimation errors. In the clockwise circuit, during the first time slot T_1 node *A* generates a sinusoid signal with initial phase ϕ_A and sends it to node *B*. Upon receiving the signal, during time slot T_2 node *B* computes the phase estimate of the received signal, generates a *periodical extension* of the signal received in T_1, and sends it to node *C*. Upon receiving the signal, node *C* repeats the estimation-and-relay operation until the final signal reaches node *A*. In the second session, node *A* generates a sinusoidal signal with initial phase ϕ'_A and transmits it along the anticlockwise circuit. After the two sessions end, each node obtains two estimates, one from the clockwise transmission and the other from the anticlockwise transmission. The sum of two estimates at each node is the same: $\Phi_A = \Phi_B = \Phi_C = \phi_A + \phi'_A + \theta_{AB} + \theta_{BC} + \theta_{CA}$ **mod** 2π.

Step 2: Measurement quantization. Different from RSS-based schemes, channel-phase-based schemes adopt a quantization approach that employs the uniformness of the channel phase distribution [9, 14]. Specifically, the interval $[0, 2\pi]$ is divided into 2^N (e.g., $N = 1, 2, 3, 4$) levels

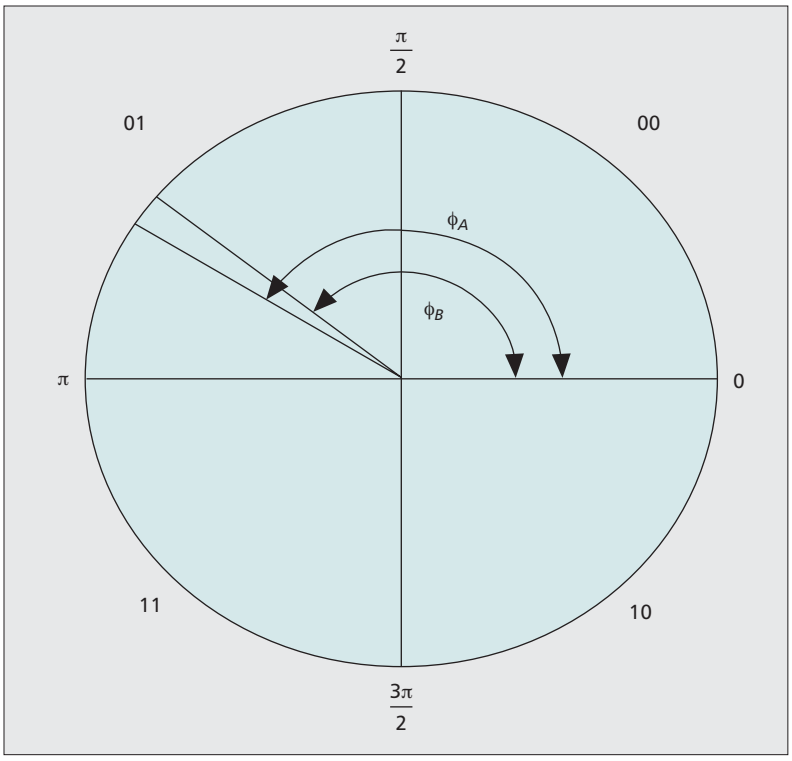


Figure 5. *An example of phase quantization with* N = *2.*

with equal length, and the quantization function is

$$Q(\Phi_i) = q \text{ if } \Phi_i \in \left[\frac{2\pi(q-1)}{2^N}, \frac{2\pi q}{2^N}\right),$$

where $q = 1, 2, \ldots, 2^N$. An example of phase quantization with $N = 2$ is shown in Fig. 5. Gray codes (one bit of error is introduced between adjacent sectors) are used to encode the quantization indices to reduce the bit discrepancies. Suppose levels 1, 2, 3, and 4 correspond to 00, 01, 11, and 10, respectively. If Φ_A and Φ_B both fall into the second level, the resulting bit vector is 01.

Step 3: Error correction. Similar to RSS-based schemes, bit discrepancies should be reconciled. In [9], the authors applied a cryptographic primitive called *secure sketch* [1] to perform the secure error correction. Note that the key reconciliation and privacy amplification techniques used in RSS-based methods are all applicable to channel-phase-based methods.

Performance Comparison

In this section, we present a comprehensive performance comparison of the existing secret key generation schemes exploiting wireless channel characteristics. The comparison is given in terms of key disagreement probability, key generation rate, key bit randomness, scalability, and implementation issues.

Key Disagreement Probability

Key disagreement probability (KDP) refers to the portion of different bits in the key bit string prior to error correction. A high KDP dramatically decreases the efficiency of the key generation protocol, and even makes the protocol fail due to the failure of key reconciliation. Experiments in [8] showed that the KDP of RSS-based schemes is determined by the variations of the wireless channel. In a stationary environment, RSS based methods have a high KDP of about 50 percent. This is because the scarcity of channel variation undermines the reciprocity of the wireless links. The enhanced RSS-based scheme in [12] has a lower KDP as the multiple-antenna system provides more mutual information for bit extraction. As shown in [9], the KDP of channel phase based schemes is constrained by the signal-to-noise ratio (SNR) and number of the nodes in the system. This is due to the fact that lower SNR and larger group size lead to phase estimation errors with larger variance. For more detailed performance evaluation, readers are referred to [8, 9].

Key Generation Rate

The basic RSS-based key generation schemes have very low-key generation rate (KGR). This is because they have to strike a balance between KGR and KDP as well as randomness of the key. First, to decrease the KDP, they have to extract only one bit out of m consecutive measurements above the upper bound or below the lower bound and discard all the other measurements. Second, KGR of the basic schemes suffers from limited level-crossing rate of the rayleigh fading channel. Oversampling the channel can produce highly correlated measurements which result in keys with low entropy [7]. The enhanced variations of RSS-based schemes have apparent improvement in KGR. In [12], multiple antennas are used to achieve a rate nearly four times larger than that of the basic methods. In [13], the proposed scheme using signal processing techniques can even achieve KGR of 22 b/s. In [9], the analytical results show that the KGR can be up to 104 b/s for a group with 6 nodes if single-tone phase estimation are used for key bit generation. This is due to:

- The random initial phase introduced in the probing signals causes the randomness of the key without only relying on fast variations of the channel.
- The use of multibit extraction is very suitable for channel-phase-based key generation schemes as channel phases are uniformly distributed.

Key Bit Randomness

A cryptographic key should be substantially random; otherwise, the adversary can crack the key with low time complexity. The randomness of a bit sequence can be measured using a National Institute of Standards and Technology (NIST) test [15]. If the p-value is greater than 0.01, it indicates the sequence is random. The randomness test results of different PHY-based key generation schemes are shown in Table 1. As discussed earlier, for the RSS-based schemes there is a trade-off between key bit randomness and key bit generation rate. That is, key bits should be extracted at different channel coherence time intervals to ensure the key bit randomness (i.e., sampling the channel at too high a

frequency produces a key with low entropy). Compared to the RSS-based methods, the channel-phase-based scheme proposed in [9] does not have such a constraint. This is because the random initial phase and channel phase both contribute to the randomness of the generated key. Even if the channel remains constant, the random initial phase can guarantee high entropy of the generated key bits.

Scalability

For applications where multiple parties are involved, a group key needs to be established for securing the group communication. Obviously, the naive method of constructing a group key is to run the pairwise key generation protocol multiple times. However, such a "centralized" group key generation protocol suffers from low efficiency when the size of the group grows. To the best of our knowledge, Wang *et al.* proposed the first efficient group key generation scheme [9]. Their scheme relies only on the transmission of periodical extensions of unmodulated sinusoidal beacons, which allows effective accumulation of channel phases across multiple nodes for secret bit generation. However, the scalability of Wang's scheme is constrained by the coherence time and SNR. On one hand, as the size of the group increases, the transmission time of the probing signals along the clockwise and anticlockwise circuits increases. Thus, a single round of bit generation should finish within the minimum coherence time; otherwise, the channel reciprocity cannot be maintained. On the other hand, both SNR and size of the group affect the KDP due to the accumulation of estimation errors. Lower SNR (i.e., less than 10 dB) or a larger group can greatly increase KDP.

Implementation Issues

The RSS-based key generation methods can use off-the-shelf hardware for implementation, as the measurement of RSS can easily be read from a wireless card on a per frame basis [7, 8]. In [12], achieving high bit generation rate requires multiple antennas to create more sources of randomness. The channel-phase-based schemes seem to have the best overall performance; however, their implementation is nontrivial. They require an analog-to-digital converter (ADC) working at Nyquist frequency of the single-tone carrier. The hardware complexity also depends on the operating frequency band of the radio system.

Conclusion

Secret key generation and distribution is essential for securing communication systems, particularly for wireless networks. As an alternative to conventional key agreement protocols, PHY-based key generation schemes can achieve information-theoretical secrecy and provide more flexibility for securing wireless networks. In this article, we provide an overview on the existing PHY-based key generation schemes exploiting the randomness of wireless channels and give a comprehensive performance comparison in terms of key disagreement probability, key generation rate, key bit randomness, scalability, and implementation issues. As discussed above, most existing studies on PHY-based key generation usually assume a passive adversary. However, a PHY-based key generation protocol may also be subject to active attacks such as modification, insertion, and jamming in practice. So far the problem of key generation in the presence of an active adversary has only received limited attention. In the future, more research efforts along this direction is needed.

	Schemes		
Tests	**Mathur *et al.* [7]**	**Jana *et al.* (mobile case) [8]**	**Wang *et al.* [9]**
Lempel Ziv Compression	1.0	N/A	1.0
Monobit Frequency	0.9910	N/A	0.8597
Runs	0.1012	0.74	0.8682
Approximate Entropy	0.8721	0.65	0.9286
Cumulative Sums (Forward)	N/A	0.34	0.9493
Cumulative Sums (Reverse)	N/A	0.89	0.8188
Block Frequency	N/A	0.38	0.8666

Table 1. *Randomness test results of different PHY-based key generation schemes. To pass the test, all* p*-values must be greater than 0.01.*

Acknowledgment

This work was partially supported by the U.S. National Science Foundation under grants CNS-0831963 and CNS-1117084.

References

[1] Y. Dodis *et al.*, "Fuzzy Extractors: How to Generate Strong Keys From Biometrics and Other Noisy Data," *SIAM J. Comp.*, vol. 38, no. 1, 2008, pp. 97–139.
[2] B. Kanukurthi and L. Reyzin, "Key Agreement from Close Secrets Over Unsecured Channels," *Proc. EUROCRYPT '09*, Apr. 2009, pp. 206–23.
[3] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Sys. Tech. J.*, vol. 28, no. 4, 1949, pp. 656–715.
[4] U. M. Maurer, "Information-Theoretically Secure Secret-Key Agreement by Not Authenticated Public Discussion," *Proc. EURO-CRYPT '97*, May 1997, pp. 209–25.
[5] A. A. Hassan *et al.*, "Cryptographic Key Agreement for Mobile Radio," *Digital Sig. Proc.*, vol. 6, 1996, pp. 207–12.
[6] B. Azimi-Sadjadi *et al.*, "Robust Key Generation from Signal Envelopes in Wireless Networks," *Proc. CCS '07*, Oct. 2007, pp. 401–10.
[7] S. Mathur *et al.*, "Radiotelepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," *Proc. MobiCom '08*, Sept. 2008, pp. 128–39.
[8] S. Jana *et al.*, "On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments," *Proc. MobiCom '09*, Sept. 2009, pp. 321–32.
[9] Q. Wang *et al.*, "Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks," *Proc. IEEE INFOCOM '11*, Apr. 2011.
[10] A. Goldsmith, *Wireless Communications*, Cambridge Univ. Press, 2005.
[11] N. Patwari *et al.*, "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *IEEE Trans. Mobile Comp.*, vol. 9, no. 1, 2010, pp. 17–30.
[12] K. Zeng *et al.*, "Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks," *Proc. INFOCOM '10*, Mar. 2010, pp. 1837–45.

[13] N. Patwari *et al.*, "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *IEEE Trans. Mobile Comp.*, vol. 9, no. 1, 2010, pp. 17–30.
[14] A. M. Sayeed and A. Perrig, "Secure Wireless Communications: Secret Keys through Multipath," *Proc. ICASSP '08*, Mar. 2008, pp. 321–32.
[15] A. Rukhin *et al.*, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," 800th Ed., NIST, May 2001.

Biographies

KUI REN [SM] (kren@ece.iit.edu) is an assistant professor in the Electrical and Computer Engineering Department at Illinois Institute of Technology. He obtained his Ph.D. degree in electrical and computer engineering from Worcester Polytechnic Institute in 2007. His research interests include network security and privacy in cloud computing, lower-layer attack and defense mechanisms for wireless networks, e-healthcare, and sensor network security. His research is sponsored by the U.S. National Science Foundationwireless security, smart grid security, and sensor network security. His research is supported by NSF, DoE, AFRL, and Amazon. He is a recipient of the NSF Faculty Early Career Development Award in 2011. He is a member of ACM.

HAI SU (hai@ece.iit.edu) received his B.E. and M.E. degrees from the University of Electronic Science and Technology of China in 2003 and 2006, respectively. He is currently a Ph.D. student in the Electrical and Computer Engineering Department at Illinois Institute of Technology. His research interests are in the areas of security and privacy in wireless networks.

QIAN WANG (qian@ece.iit.edu) received his B.E. degree from Wuhan University, China, in 2003 and his M.E. degree from Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, China, in 2006, both in Electrical Engineering. He is currently working toward a Ph.D. degree in the Electrical and Computer Engineering Department at Illinois Institute of Technology. His research interests include wireless network security and privacy, cloud computing security, and applied cryptography.