IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 3, 2015, accepted January 19, 2016, date of publication January 27, 2016, date of current version March 8, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2521718

Key Generation From Wireless Channels: A Review

JUNQING ZHANG[1], TRUNG Q. DUONG[1], (Senior Member, IEEE), ALAN MARSHALL[2], (Senior Member, IEEE), AND ROGER WOODS[1], (Senior Member, IEEE)

[1]Institute of Electronics, Communications and Information Technology, Queen's University Belfast, Belfast, BT3 9DT, U.K.
[2]Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, U.K.

Corresponding author: J. Zhang (jzhang20@qub.ac.uk)

This work was supported in part by Queen's University Belfast University Studentships, in part by the Royal Academy of Engineering Research Fellowship under Grant RF1415/14/22, in part by the U.S. Ireland Research and Development Partnership Department for Employment and Learning, U.K., within a grant involving Rice University, USA, University College Dublin, Ireland, through the WiPhyLoc8 Project under Grant USI033, and in part by the Newton Institutional Links under Grant 172719890.

ABSTRACT Key generation from the randomness of wireless channels is a promising alternative to public key cryptography for the establishment of cryptographic keys between any two users. This paper reviews the current techniques for wireless key generation. The principles, performance metrics and key generation procedure are comprehensively surveyed. Methods for optimizing the performance of key generation are also discussed. Key generation applications in various environments are then introduced along with the challenges of applying the approach in each scenario. The paper concludes with some suggestions for future studies.

INDEX TERMS Physical layer security, key generation, wireless communication.

I. INTRODUCTION

A. WIRELESS NETWORK SECURITY

The inherent broadcast nature of wireless communication allows transmissions to be received by any user within the range, resulting in attackers' ability to initiate various passive attacks such as eavesdropping, traffic analysis and monitoring, etc, or to execute active attacks like jamming, spoofing, modification, replaying and denial-of-service (DoS) attack, etc. [1].

There has been extensive research interest to protect wireless transmission [2]. Traditionally, the data is secured by classic encryption schemes [3], [4], which work on the assumption that the algorithm is complex enough so that the time taken by eavesdroppers to crack the cryptographic system is much longer than the validity of the information itself, therefore, the backward secrecy is guaranteed. As shown in Fig. 1, classic encryption schemes consist of symmetric encryption schemes and asymmetric encryption schemes, depending on the keys that the two cryptographic parties use. Symmetric encryption schemes use the same key and are usually employed for data protection thanks to their efficiency in data encryption. Asymmetric encryption schemes, also known as public key cryptography, use the same public key but different private keys and are usually applied for key distribution. An illustration of a classic encryption system is shown in Fig. 2a, where Alice and Bob represent two legitimate users who want to share information securely between each other.

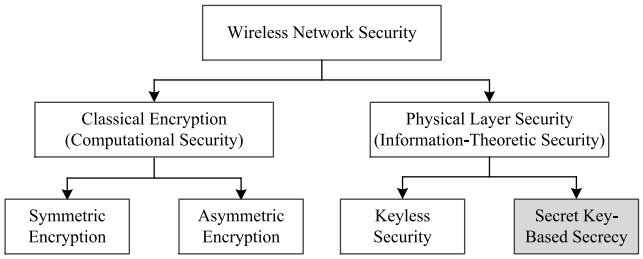

FIGURE 1. Research streams in wireless network security.

Classic encryption schemes are faced with several vulnerabilities. Take public key cryptography as an example. Firstly, it depends on the computational hardness of some mathematical problems, e.g., discrete logarithm. This computational security nature may not hold in future due to the rapid development of hardware technology. In addition, it requires a key management infrastructure which should be secured as well. This approach is therefore less attractive for many wireless sensor networks (WSNs) and ad hoc networks applications, because sensor nodes have limited computational capacity while ad hoc networks are decentralized.

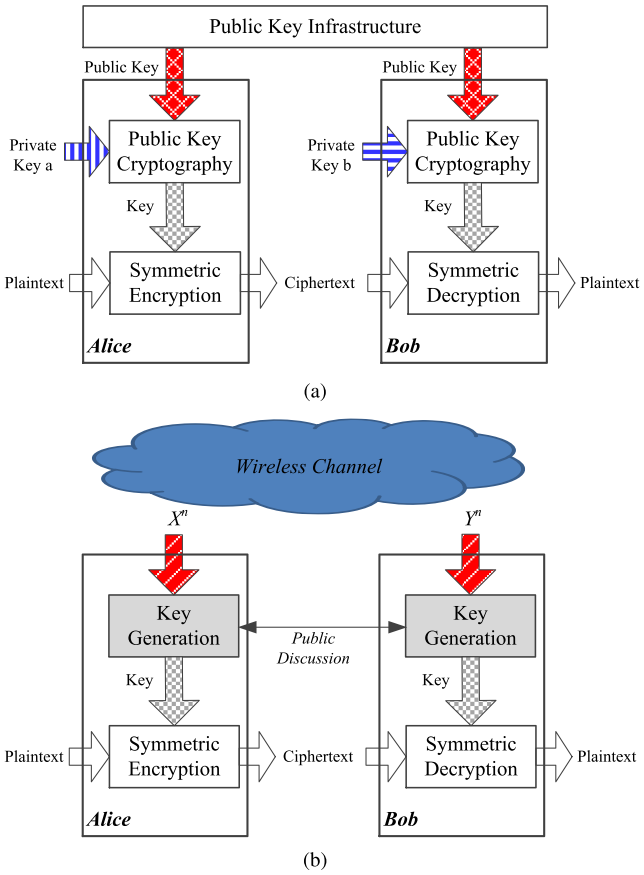

FIGURE 2. Illustration of wireless network security systems. (a) Illustration of a classic encryption system. Information exchange between public key cryptography modules is omitted for brevity. (b) Illustration of a key generation-based hybrid cryptosystem.

While classic encryption schemes are applied in the upper layers of the communication protocols, the physical layer can also be exploited to enhance wireless security. Physical layer security (PLS) schemes leverage unpredictable and random characteristics of wireless channels in order to achieve information theoretic-security [5]–[10]. As shown in Fig. 1, PLS schemes are composed of keyless security and secret key-based secrecy [8]. Pioneered by Wyner's wiretap channel model [11], keyless security does not require keys for encryption but employs code design and channel properties of legitimate users and eavesdroppers to achieve secrecy (see [8] and references therein). However, the legitimate users usually require full/part of instantaneous/statistical channel state information (CSI) of the eavesdroppers, which is not always available in practice and results in a very complex implementation.

Secret key-based secrecy dated back as early as 1919 when the concept of one-time pad, also known as Vernam cipher [12], was used to encrypt each message bit with a random secret key bit. Later on, Shannon laid the theoretical basis for perfect secrecy [13]. The message M is encoded into codeword C which does not reveal any information about the message, i.e.,

$$H(M|C) = H(M), \tag{1}$$

where $H(\cdot)$ denotes the entropy. This requires the information of the key sequence should be larger than, or at least equal to, the information of the message. One possible way to establish the key is to generate keys from the wireless channels. However, in practice, it is very challenging, if not impossible, to efficiently establish random keys between legitimate users which cannot be reused. Alternatively, a hybrid cryptosystem can be constructed by combining key generation and symmetric encryption, as illustrated in Fig. 2b. The security level of the system is enhanced by replacing public key cryptography with key generation.

B. KEY GENERATION

In this paper, we review secure key generation from the randomness of wireless channels. Unlike the computationally secure nature of the public key cryptography, wireless key generation is information-theoretically secure, because it is based on the random characteristics of wireless channels [14], [15]. In addition, this technique is lightweight and does not require any aid from other users. A comparison of the above mentioned schemes is given in Table 1.

Key generation was theoretically proposed/investigated in [14] and [15] in 1993. Key generation model is shown

TABLE 1. Comparison of security schemes.

Scheme	Description	Implementation	Complexity	Pros	Cons
Symmetric encryption	Legitimate users use the same key to encrypt data.	Yes	Low	Efficiency in data encryption	Computationally secure; A secure key required prior.
Asymmetric encryption	Legitimate users use the same public key but different private keys to distribute a session key.	Yes	High	Key distribution with different private keys	Computationally secure; Public key infrastructure required; Not applicable to low computational capacity devices.
Keyless security	Legitimate users securely communicate by leveraging code design and channel properties.	Not reported	High	Information-theoretically secure; Secret transmission without keys.	Eavesdroppers' CSI usually required.
Key generation	Legitimate users generate key from the randomness of the common channel.	Yes	Low	Information-theoretically secure; Lightweight; No aid from other users required.	Limited by the channel dynamicity.

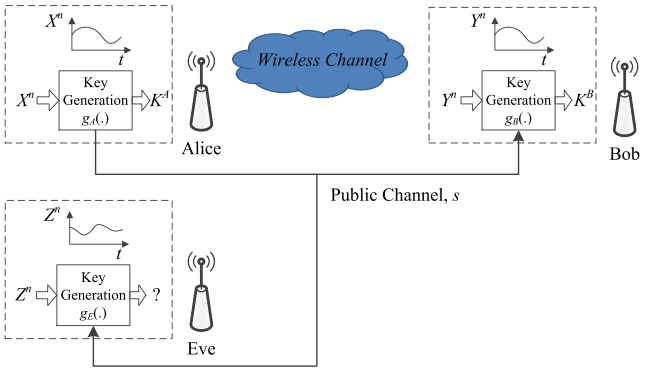

FIGURE 3. Key generation model.

in Fig. 3, where Alice and Bob want to establish a secure cryptographic key and an eavesdropper Eve located d-cm away from Alice, listens to all the transmissions. Alice, Bob and Eve can get correlated observations $X^n = (X_1, ..., X_n)$, $Y^n = (Y_1, ..., Y_n)$ and $Z^n = (Z_1, ..., Z_n)$, respectively. Alice and Bob will exchange a message s over the public channel, which may be heard by Eve as well. For any $\epsilon > 0$ and sufficiently large n, if there exists $K^A = g_A(X^n, s)$ and $K^B = g_B(Y^n, s)$ making the key generation system satisfy

$$\Pr(K^A \neq K^B) < \epsilon, \tag{2}$$

$$\frac{1}{n} I(K^A; s, Z^n) < \epsilon, \tag{3}$$

$$\frac{1}{n} H(K^A) > R - \epsilon, \tag{4}$$

$$\frac{1}{n} \log |\mathcal{K}| < \frac{1}{n} H(K^A) + \epsilon, \tag{5}$$

then R in (4) is the achievable key rate, where $I(\cdot)$ denotes mutual information and $\mathcal{K}$ is key's alphabet. (2) means that Alice and Bob can generate the same key with a high probability; (3) indicates the message exchange via public discussion leaks no information to Eve, which guarantees the security of the generated key; (5) ensures the key is uniformly distributed, which is desirable for the cryptographic applications. The largest achievable key rate is defined as key capacity and given as

$$C_K = \min[I(X; Y), I(X; Y|Z)]. \tag{6}$$

There has been extensive research effort to implement the above theory in practice and to approach to the theoretical limits. The first practical key generation protocol was proposed in 1995 [16] and since then has triggered research interest in wireless key generation. Chapter 4 in [7] reviewed the wireless key generation from the information theory perspective. The authors in [17] surveyed the key generation development merging channel probing and quantization as one step, which is shown later as two separate ones. We note that a recent study in [18] has introduced the challenges and opportunities of the key generation but it has not considered implementation details. Although in [19], key generation schemes have been summarized, e.g., received signal strength (RSS)-based and channel phase-based schemes, a thorough review of key generation techniques is still needed as these schemes and techniques have evolved fast since then. In this paper, we provide a literature review on techniques of key generation systems. We also highlight research areas of key generation that need more understanding and provide suggestions for future research.

The rest of the paper is organized as follows. Section II and III introduce the key generation principles and evaluation metrics, respectively. Section IV details the channel parameters that can be used for key generation, including CSI and RSS. The key generation procedure is explained in Section V and optimized in Section VI. Applications in various environments are then reviewed in Section VII. Section VIII concludes the paper with future research suggestions.

II. KEY GENERATION PRINCIPLES

Key generation is based on three principles, i.e., *temporal variation*, *channel reciprocity*, and *spatial decorrelation*.

Temporal variation is introduced by the movement of the transmitter, receiver or any objects in the environment, which will change the reflection, refraction and scattering of the channel paths. The randomness caused by such unpredictable movement can be used as the random source for key generation [20]–[26]. There is research effort to exploit the randomness in frequency domain [27]–[31] and spatial domain [32]–[36]. However, in a static environment where these features remain the same, the randomness is rather limited. Temporal variation is thus still required in order to introduce a sufficient level of randomness. It can be quantified by the autocorrelation function (ACF) of the signal, which is given as

$$R_X(t, \Delta t) = \frac{E\{(X(t) - \mu_X)(X(t + \Delta t) - \mu_X)\}}{\sigma_X^2}, \tag{7}$$

where $E\{\cdot\}$ denotes the expectation operator, and μ_X and σ_X represents the mean value and standard deviation of random variable $X(t)$, respectively.

Channel reciprocity implies that the multipath and fading at both ends of the same link, i.e., same carrier frequency, are identical which is the basis for Alice and Bob to generate the same key. The signals have to be measured by hardware platforms, which usually work in half duplex mode and introduce noise. Therefore, the received signals of the uplink and downlink path are asymmetric due to the non-simultaneous measurements and noise effects, which limits key generation applications within time-division duplexing (TDD) systems and slow fading channels. These effects can be mitigated using signal processing algorithms discussed in Section V-A. The signal similarity can be quantified by the cross-correlation between the measurements, which is given as

$$\rho_{XY} = \frac{E\{XY\} - E\{X\}E\{Y\}}{\sigma_X \sigma_Y}. \tag{8}$$

Spatial decorrelation indicates that any eavesdropper located more than one half-wavelength away from either user

experiences uncorrelated multipath fading, which can also be described by the cross-correlation between the signals of legitimate users and eavesdroppers. This property is essential for the security of key generation systems and has been claimed in most key generation papers. However, it may not be satisfied in all the environments. Channel variation is contributed by large-scale fading (i.e., path loss and shadowing) and small-scale fading [37]. In the Jake's model with a uniform scattering Rayleigh environment and without a line-of-sight (LoS) path, if the number of scatters grows to infinity, the signal decorrelates over a distance of approximately one half-wavelength [37]. Some experiments have also shown this property [38]–[41]. However, when large-scale fading is dominant, special attention is required as the channel is more correlated [42]. There is research reporting that signals observed by eavesdroppers are correlated to signals of legitimate users [43]–[45], which makes key generation systems vulnerable and requires special consideration to combat eavesdropping. In general, spatial decorrelation has not been extensively studied and is worth more research input.

III. PERFORMANCE METRICS

Key generation is designed to establish cryptographic keys for encryption and/or authentication. These applications have special requirements on the key's randomness, refresh rate, etc. Thus, key generation systems can be correspondingly evaluated in terms of three important metrics: randomness, key generation rate (KGR), and key disagreement rate (KDR).

A. RANDOMNESS

Randomness is the most important feature of key generation systems. Cryptographic applications have strict requirements on the randomness of the key sequence [4]. A statistical randomness test suite provided by National Institute of Standards and Technology (NIST) [46] is widely used to test the randomness of random number generators (RNGs) and pseudo random number generators (PRNGs). In essence, a key generation system is a type of RNG, so NIST statistical test suite can also be applied.

As randomness is a probabilistic property, statistical analysis is employed to test a specific *null hypothesis* (H0), i.e., the sequence under test is random. A *P-value* is returned by each test, which summarizes the strength of the evidence against the null hypothesis. A significance level α, typically in the range $[0.001, 0.01]$, is chosen. When $P\text{-}value \geq \alpha$, the sequence is accepted as random, otherwise, it is deemed to be non-random.

There are infinite statistical features of a random sequence, therefore, in practice, it is impossible to test all the features using a finite set of tests [46]. The NIST test suite has 15 tests to evaluate different randomness features, each for a specific feature of the randomness, e.g., the proportion of 1s and 0s (frequency test), periodic feature (DFT test), etc. Some tests require extremely long sequence. For example, the recommended input length is 10^6 for the linear complexity, random excursions and random excursions variant tests and is judged to be very long in a key generation system. Thus, most of the key generation research has only adopted a subset of the randomness tests to assess a subset of the randomness features [20], [21], [23], [30], [47]–[50].

The readers are referred to [46] for a detailed description of all the randomness tests and advised to download the source code of the test suite to evaluate the randomness of their key generation systems.

B. KGR

KGR describes the amount of secret bits produced in one second/measurement. It mainly depends on environment conditions, which determines the amount of randomness available for extraction. A high KGR is essential for the real time key generation process as the cryptographic schemes require a certain length of keys. For example, advance encryption standard (AES) needs a key sequence with a minimum length of 128 bits.

C. KDR

KDR is the percentage of the different bits between the keys generated by Alice and Bob, which is defined as

$$KDR = \frac{\sum_{i=1}^{N} |K^A(i) - K^B(i)|}{N}, \tag{9}$$

where N is the length of keys. The KDR should be smaller than the correction capacity of information reconciliation techniques, otherwise, key generation fails, which is discussed in Section V-C.

D. SUMMARY

There are also other assessment metrics such as scalability and implementation issues [19]. However, randomness, KGR and KDR are the most important and popular metrics which describe the success and efficiency of the system, which are therefore used for evaluation throughout this paper.

IV. CHANNEL PARAMETERS

Channel parameters are the most essential part of key generation, as it is the random source representing unpredictable channel characteristics. In this section, CSI and RSS are reviewed.

A. CSI

CSI is a fine-grained channel parameter which provides detailed channel information. CSI-based systems are able to provide a high KGR [51] and have been experimentally proved to be immune to predictable channel attacks [30]. In this paper, CSI mainly refers to channel impulse response (CIR) and channel frequency response (CFR).

1) CIR

A multipath channel can be modelled as several resolvable path components and its CIR $h(\tau, t)$ can be given as

$$h(\tau, t) = \sum_{l=0}^{L(t)} \alpha_l(t) e^{-j\phi_l(t)} \delta(\tau - \tau_l(t)), \tag{10}$$

where $\alpha_l(t)$, $\phi_l(t)$ and $\tau_l(t)$ are the amplitude attenuation, phase shift and time delay of the l^{th} tap, respectively, $L(t)$ is the total path number and $\delta(\cdot)$ is the Dirac function.

CIR has been proved to be ideal for key generation [51]. It has both amplitude and phase information. In wideband systems, the phase shift $\phi_l(t)$ can be estimated and used for key generation [52]–[55]. It can also be used in narrowband systems [29], [47], [48], but the phase in this case is decreased into a single-dimension parameter which loses lots of channel information. Phases can be accumulated to each other and this special feature leads to interesting applications such as group and cooperative key generation [47], [48]. In addition, phases of all the paths are distributed uniformly on $[0, 2\pi]$, which are not affected by the path power. There is only one practical phase-based key generation system implemented in a narrowband system [29] and no practical wideband-based systems have been reported yet. This is because phase is vulnerable to noise, carrier frequency offset and asynchronous clocks/clock drift at the receiver, etc.

Another aspect is amplitude of CIR. In an ultra wideband (UWB) system, the amplitude can be estimated by sending a pulse signal [39], [40], [56]–[59]. The UWB-based measurement systems are usually constructed by oscilloscope, waveform generator, etc. In a narrowband system when the transmission power is fixed, the amplitude of CIR is equivalent to the received power [29]. The power of CIR decreases with delay, e.g., it follows exponential distribution in an indoor environment, resulting in a high KDR for the paths with small power as they are vulnerable to the noise. This may be tackled by using the peak CIR only [20] which sacrifices the KGR, or using an adaptive quantization algorithm [58].

2) CFR

CFR provides channel effect in frequency domain and can be given as

$$H(f, t) = \int_0^{\tau_{\max}} h(\tau, t) e^{-j2\pi f \tau} d\tau, \tag{11}$$

where $\tau_{\max}$ is the maximum channel delay. Channel estimation in orthogonal frequency-division multiplexing (OFDM) systems can get a noisy observation of CFR [60]–[63], which can be written as

$$\widehat{H}(f, t) = H(f, t) + \widehat{w}(f, t), \tag{12}$$

where $\widehat{w}(f, t)$ is the noise effect in frequency domain.

CFR-based systems have been mostly implemented in IEEE 802.11 OFDM systems [30], [31], [64], [65], as it is convenient to extract channel estimation. Only the amplitude of the channel estimation is used in practical implementation [30], [31], [65] as the phase estimation is usually impacted by the time and frequency offset. CFR may also be estimated by comparing the frequency spectra of the transmitted and received signal [66]. Unlike the CIR, the powers of the channel responses of all the frequencies are identical in an uncorrelated scattering environment [51], which is beneficial for the improvement of KGR [30], [31].

Channel estimation information is not available in most WiFi network interface cards (NICs) with the current exception of Intel WiFi Link 5300 wireless NIC [67]. Customized hardware platforms are also able to provide CSI, such as universal software radio peripheral (USRP) [68] and wireless open-access research platform (WARP) [69].

B. RSS

The transmitted signal $x(t)$ experiences the multipath channel and the received signal can be written as

$$y(t) = \int_0^{\tau_{\max}} h(\tau, t) x(t - \tau) d\tau + n(t), \tag{13}$$

where $n(t)$ is the noise effect. The instantaneous power of the signal $|y(t)|^2$ is usually not reported by NICs and transceivers. However, the average power level is usually available and referred as RSS.

RSS is currently the most popular channel parameter used in key generation, especially for practical implementation due to its availability. Most RSS-based key generation systems are applied either in IEEE 802.11 systems [20]–[22], [50], [70] or in IEEE 802.15.4 systems [23]–[27], [71].

RSS is a coarse-grained channel information metric and only one RSS value can be obtained from each packet, which limits the KGR. In addition, RSS is vulnerable to predictable channel attacks [21], [29]. What's more, whilst there are lots of practical implementations, the theoretical modelling and analysis of RSS has not been reported yet. Finally, RSS may be interpreted in different ways, which requires special attention when the devices are provided by different manufacturers [21], [70], [72].

C. SUMMARY

CIR $h(\tau, t)$ is the intrinsic random source for both CSI-based and RSS-based key generation systems. The parameters measured by users may be different but are always a function of $h(\tau, t)$.

The selection of the channel parameters for key generation will mainly be determined by the wireless techniques adopted. For example, RSS is available in all wireless systems, including systems modulated by direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS). The signal power is quite small in UWB systems but the CIR can be measured through the pulse transmission. A summary and comparison of key generation applications in different wireless networks is given in Table 2.

TABLE 2. Key generation applications in wireless networks.

Technique		Modulation	Parameter	Features	Testbed	Representative Work
IEEE 802.11	n	MIMO OFDM	RSS, CSI	MIMO OFDM enables CSI measurements in both frequency and spatial domains	RSS: all NICs; CSI: Intel 5300 NIC, and customized hardware platforms, such as USRP [68] and WARP [69]	RSS-based: [22] CSI-based [30], [31]
	a	OFDM	RSS, CSI	OFDM enables CSI measurements in frequency domain		RSS-based: [20], [21], [50], [70] CSI-based: [65]
	g	OFDM, DSSS	RSS, CSI			
	b	DSSS	RSS	RSS available		
IEEE 802.15.4		DSSS	RSS	Widely used in WSN; Sensor motes are powered by battery and with low computational capacity; Usually low mobility.	MICAz [73], TelosB [74]	[23]–[27], [71]
Bluetooth		FHSS	RSS	FHSS allows sampling RSS in different frequencies.	Smartphones	[75]
UWB		Pulse	CIR	Low power, large bandwidth ($>$ 500 MHz)	Constructed by oscilloscope, waveform generator, etc	[39], [40], [56]–[59]
LTE		MIMO OFDM	RSS, CSI	Only applied in slow fading channel for key generation; Ability to adjust parameters, such as power allocation; No practical implementation reported yet.	Smartphones	[76]

V. KEY GENERATION PROCEDURE

Key generation procedure can be divided into four stages: *channel probing*, *quantization*, *information reconciliation*, and *privacy amplification*, as summarized in Table 3 and illustrated in Fig. 4. One user serves as the initiator, and the other as the responder. Without loss of generality, Alice is selected as the initiator. In order to simplify the flow chart, the stage synchronization between Alice and Bob is not shown.

A. CHANNEL PROBING

Channel probing is the key step to harvest the randomness from channel which requires two users to alternately measure the common channel through the received signals. As shown in Fig. 4, at time $t_{i,A}$, Alice transmits the i^{th} probing signal to Bob who will measure some channel parameter through the received signal and store it in Y_i'. At time $t_{i,B}$, Bob transmits his i^{th} probing signal to Alice who will also measure the same channel parameter and store it in X_i'. The sampling time difference $\Delta t_i = |t_{i,A} - t_{i,B}|$ is deliberately kept smaller than the channel coherence time so the channel during the two probes can be regarded as constant. Alice and Bob will repeat the above process until sufficient results are collected.

Research in channel probing mainly considers channel parameter, signal pre-processing, and channel probing rate. The channel parameters valid for key generation have already been discussed in Section IV. Although the channel features at each end of the link are reciprocal, the measured received signals are asymmetric mainly due to non-simultaneous measurements (i.e., $\Delta t_i \neq 0$) and the independent noise residing in the two separate hardware platforms. Therefore, signal pre-processing is used to improve the cross-correlation between the received signals, i.e., $X_i = f(X_i')$ in Fig. 4.

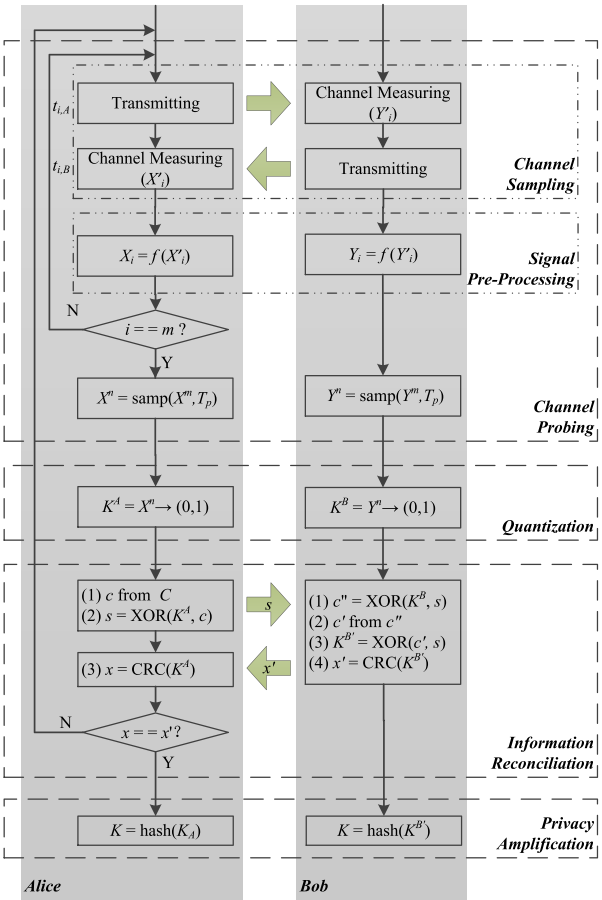

FIGURE 4. Key generation procedure.

The effects of non-simultaneous measurements and noise can be mitigated by interpolation [23], [24] and filtering [25], [30], [49], [77], [78], respectively.

TABLE 3. Key generation procedure.

Stage	Purpose	Research Problems
Channel probing	Channel measurements through the received signals.	• Channel parameters: The granularity of the chosen parameter determines the sampling efficiency. • Signal pre-processing: Improving signals' cross-correlation by interpolation and/or filtering. • Channel probing rate: Removing redundancy between the measurements.
Quantization	Conversion of channel measurements into binary values	• Selection of the threshold and quantization level. • Performance optimization between randomness, KGR and KDR.
Information reconciliation	Reconciliation of the mismatch bits between Alice and Bob using protocols or error correction codes	• Optimization between the correction capacity and information leakage.
Privacy amplification	Removal of information revealed in information reconciliation stage	• Cross design with information reconciliation. • Determination of the amount of leaked information.

There may be redundancy within the sampled measurements X^m and Y^m, which are therefore resampled by a probing rate T_p, chosen to be larger than the coherence time. An optimal probing rate is determined based on the modelling of the ACF of the signal [64] when the channel is changing in the same rate. However, the channel randomness is caused by unpredictable movement, leading to different change rate of the channel condition. A fixed probing rate results in potential problems such as inefficient probing when the channel changes fast or redundancy between the samples when the channel changes slowly. Therefore, a proportional-integral-derivative (PID) controller-based adaptive probing system has been designed to tune the probing rate according to the channel conditions [79], which could generate key sequences both securely and effectively in a dynamically changing environment. Channel phase-based system in [47] does not suffer from the above problem as it can probe each other continuously. This is because besides the phase shift incurred by the channel, there is also a random initial phase introduced at each side, which is not affected by the channel coherence time.

B. QUANTIZATION

Similar to an analog-to-digital converter (ADC), quantization in key generation is also a method to map the analog channel measurements into binary values. The quantization level QL in key generation has the same meaning as in ADC, which is the number of key bits quantized from each measurement. Due to the discrepancy between received signals of any two users, the quantization level is adjusted according to the signal-to-noise ratio (SNR) of the channel. In multi-bit quantization, Gray coding may be used in order to reduce the key disagreement.

The thresholds are the reference levels used to divide the measurements into different groups. Mean value μ (or together with standard deviation σ) [20], [21] and cumulative distribution function (CDF) [24] are commonly used to determine the thresholds. Mean value and standard deviation-based quantization scheme has simple implementation. The thresholds are determined as

$$\eta+ = \mu + \alpha \times \sigma; \tag{14}$$

$$\eta- = \mu - \alpha \times \sigma. \tag{15}$$

When $\alpha \neq 0$, the measurements between $\eta+$ and $\eta-$ will be dropped. The samples above $\eta+$/below $\eta-$ will be converted to 1/0. The CDF-based quantizer is detailed in Algorithm 1, which is more flexible as it can be designed as multi-bit quantizer. In addition, its thresholds can be tuned to guarantee the same proportion of 0s and 1s, an important feature for the randomness.

In essence, the quantizer design is the adjustment of the quantization level and threshold in order to approach an optimal performance of the randomness, KGR and KDR. This results in different design variations, e.g., adaptively adjusting the threshold in order to follow the slow variation of

Algorithm 1 CDF-Based Quantization Algorithm

1: $F(x) = \Pr(X^n < x)$
2: $\eta_i = F^{-1}(\frac{i}{2^{QL}}), i = 1, 2, ..., 2^{QL} - 1$
3: $\eta_0 = -\infty$
4: $\eta_{2^{QL}} = \infty$
5: Construct Gray code b_i and assign them to different intervals $[\eta_{i-1}, \eta_i]$
6: $K(j, QL) = b_i$, if $\eta_{i-1} \leq X_j < \eta_i$

the signal and finally avoiding long 1s or 0s and improving the randomness feature [21]; multi-bit quantization for a higher KGR [24]; dropping bits which are not all at the same side of the threshold for a better agreement [20]. Performance evaluation and comparison of the quantization schemes can be found in [41], [80].

C. INFORMATION RECONCILIATION

Although signal pre-processing algorithms can be adopted to improve the cross-correlation of the channel measurements, there may still be key disagreement between Alice and Bob after quantization. The mismatch can be corrected using information reconciliation techniques, which can be implemented with protocols such as Cascade [21], [49], [79], [81] or error correcting code (ECC) like low-density parity-check (LDPC) [51], [82], [83], BCH code [84], [85], Reed-Solomon code [86], Golay code [23], [26], [29], and Turbo code [87], etc. ECC-based reconciliation schemes are more efficient than Cascade, but they also leak more information [81] and have higher complexity [7]. The selection of the ECC depends on the complexity and correction capacity. For example, the maximum correction capacity rate of $[n, k, t]$ BCH code is given as

$$\zeta = \frac{t_{max}}{n} = \frac{2^{m-2} - 1}{2^m - 1}, \tag{16}$$

which approaches 0.25 when m becomes large.

Secure sketch [84] is introduced as an example, which is also illustrated in Fig. 4. An ECC C is adopted to correct the disagreement. Alice first randomly selects a codeword c from C and then calculates s by exclusive OR-ing her key sequence K^A with c, i.e., $s = \text{XOR}(K^A, c)$, which is then sent to Bob by the public channel. Bob will calculate c'' by exclusive OR-ing his key sequence K^B with the correctly received s, i.e., $c'' = \text{XOR}(K^B, s)$, and decode c' from c''. He calculates $K^{B'}$ by exclusive OR-ing c' with s, i.e., $K^{B'} = \text{XOR}(c', s)$. When the Hamming distance between c and c'' is smaller than the correction capacity t of the correction code, i.e., $dis(c - c'') < t$, Bob can agree on the same key as Alice, i.e., $K^{B'} = K^A$.

The key agreement can be confirmed by implementing cyclic redundancy check (CRC) or other protocols and tools, e.g., automated validation of Internet security protocols and applications (AVISPA) software was used in [57]. There will be a risk that the KDR exceeds the correcting capacity rate of the information reconciliation which results in a failure and restart of the entire key generation process from channel probing.

D. PRIVACY AMPLIFICATION

Some information is transmitted publicly in the information reconciliation stage, which can be heard by the eavesdropper as well. This can potentially compromise the security of the key sequence. Privacy amplification is then employed to remove the revealed information from the agreed key sequence at Alice's and Bob's side [88]. This can be implemented by extractor [47], or universal hashing functions, such as leftover hash lemma [21], [50], cryptographic hash functions (e.g., secure hash algorithm) [86], [87], and Merkle-Damgard hash function [79].

Privacy amplification and information reconciliation always appear together, which requires a cross design between these two stages. However, in practice, it is difficult to quantify the amount of the leaked information, or to identify where the leakage occurs in the data.

E. SUMMARY

The key generation implementation is usually low cost, as it only requires non-complex operations, e.g., sampling and storing data in the channel probing stage. All these operations can be implemented using the off-the-shelf hardware, with only a change to the drivers.

The key generation procedures vary according to the system implementation. All the key generation systems need channel sampling and quantization while information reconciliation and privacy amplification may be not applied due to specific implementation and environment where the systems achieve perfect agreement after quantization [20], [25].

VI. PERFORMANCE OPTIMIZATION

The design criterion of key generation systems is to attain an optimal performance, which can be achieved by a careful consideration of the key generation stages.

KGR can be improved by the appropriate selection of channel parameter, channel probing rate, and quantization scheme, etc, which are summarized as follows:

- Randomness extraction from the fine-grained CSI [30], [31], [51], [64].
- More channel information extraction by leveraging multiple antenna diversity [22], [32];
- Introduction of relay nodes in order to make use of the channel information between the users and the relay nodes [48], [89]–[91];
- Employment of random initial phase in order to achieve multiple probes in one coherence time [47];
- Adaptive channel probing [79];
- Multi-bit quantization [21], [24];

The above methods can also be combined to further improve the KGR if the system permits. For example, a MIMO OFDM system can extract keys very efficiently as it is able to measure the CSI using multiple antennas [30].

The KDR will usually be high if the sampled channel parameters are quantized directly, especially in low SNR environments. The KDR can be reduced with the aid of the signal processing algorithms discussed in Section V-A and using a more robust quantization algorithm such as level crossing [20]. A KDR comparison of different quantization schemes can be found in [41], [80].

The three evaluation metrics, i.e., randomness, KGR, and KDR, contradict each other. For example, a fast probing rate will produce a high KGR but may result in temporal

TABLE 4. Comparison of key generation systems.

Representative Work	Technique	Testbed	Parameter	KGR	KDR
Liu *et al.* [30]	Fine-grained channel information; Multi-bit quantization (3-bit); MIMO (2×2).	Laptop with Intel WiFi Link 5300 NIC	CSI	360 bit/pkt	8%
Zeng *et al.* [22]	Multiple antenna diversity	Laptop with Intel WiFi Link 5300 NIC	RSS	10 bit/s[1]	10%
Wei *et al.* [79]	Adaptive channel probing	Laptop with Atheros NIC	RSS	100 bit/s	N/A
Patwari *et al.* [24]	Multi-bit adaptive quantization	TelosB sensor mote	RSS	$10 \sim 22$ bit/s	$0.54\% \sim 2.2\%$
Mathur *et al.* [20]	Level crossing algorithm[2]	Customized platform	CIR	1.17 bit/s ($m = 4$)	$15.85\% \sim 10^{-7}$ ($m = 2 \sim 11$, SNR = 30 dB)
		Laptop with Atheros NIC	RSS	1.3 bit/s ($m = 4$)	
Ali *et al.* [25]	Channel sampling using regular data transmission; Employing Savitzky-Golay filter to mitigate noise effect.	MICAz sensor mote	RSS	$0.037 \sim 0.205$ bit/s	$0 \sim 1.6\%$

[1] KGR of a multiple antenna system (3×3 antenna pairs) is 4.5 higher than the KGR of a single antenna system
[2] Level crossing algorithm requires a parameter m, which is the number of the same consecutive bits in an excursion.

redundancy and compromise the randomness. A bigger quantization level can also produce a higher KGR, however, it may lead to a larger KDR especially in low SNR environments. Randomness usually cannot be compromised. Therefore, when designing a key generation system, a relatively optimal tradeoff should be achieved between KGR and KDR according to the system requirements and environments. For example, the KDR in [20] can be kept as low as 10^{-8} by adjusting the parameters in their level crossing algorithm but the KGR will be very small. A comparison of selected key generation systems in terms of techniques and performance is given in Table 4.

VII. APPLICATION SCENARIOS

Key generation has already been prototyped in several different areas. In this section, a review of applications in different environments is carried out and the challenge of each environment is discussed.

A. WIRELESS LOCAL AREA NETWORKS (WLANs)

WLAN connectivity is now incorporated into most laptops, tablets and smartphones, making it the most popular wireless access technology. The main WLAN standards are IEEE 802.11 a/b/g/n operating in 2.4 GHz and 5 GHz bands. Due to its wide availability, many practical key generation implementations in WLAN have been reported. WLAN is primarily designed for indoor environments, where there is limited mobility. Therefore, in order to guarantee the randomness of the key sequence, the probe rate should be relatively large, as the channel can remain essentially static over long periods, which results in a low KGR.

RSS is available in all the WLAN standards and can be obtained in the commercial NICs. The research emphases are mainly on the improvement of KGR and decrease of KDR. For example, KGR is increased with the aid of multi-antenna [22] or adaptive channel probing [79], and KDR can be decreased by using a level crossing algorithm [20].

CSI-based systems are also feasible as IEEE 802.11 a/g/n use OFDM modulation and channel estimate can provide detailed channel information. Practical systems have been implemented using Intel WiFi Link 5300 wireless NIC and the KGR is much higher than RSS-based systems [30], [31]. The channel responses of individual OFDM subcarriers have also been leveraged for key generation [65] and an optimal probing rate can be tuned based on its theoretic model [64].

B. WIRELESS SENSOR NETWORKS (WSNs)

WSNs are widely used in environment monitoring, health care, or military [92], where there is a clear need to protect the data exchanged. The sensor nodes in WSNs are equipped with 802.15.4 transceivers operating in the 2.4 GHz to 2.8 GHz industrial, scientific and medical (ISM) band. RSS information is usually available in these transceivers and can be used to establish the keys in WSNs. However, the sensor nodes are static or with little movement, battery powered, and with low computational capacity, which places special requirements on the implementation. A key generation architecture for resource-constrained devices is proposed in [93].

In order to address the issue of the static nature of channel in WSN, randomness in the frequency domain is exploited [27]. The key generation system is designed to probe on different channels in order to extract the randomness from the frequency-selective fading. Signals with different carrier frequencies experience varied fading and thus the RSSs are different. However, this method requires a frequency-selective channel and the randomness is rather limited. After the initial generation from the randomness introduced by frequency selectivity, the refresh of the key becomes impossible if there is no further randomness caused by the movement or other changes to the wireless channel.

Body area network is a special application of WSN with sensors mounted on the body [94]. An RSS-based key generation system is implemented in body area networks [25].

In order to save energy, channel is sampled in the course of a routine transmission rather than dedicated communications. A Savitzky-Golay low pass filter is employed to mitigate the noise component so the system can achieve a high key agreement rate around 98%, or even 100% with a specific setting. Thus there is no information reconciliation and specific communication in their system. This is at the cost of very low KGR. It takes 15 to 35 minutes to generate a 128-bit key.

C. VEHICULAR COMMUNICATION

As discussed in Section V-A, when $|t_{i,A} - t_{i,B}|$ is much smaller than the coherence time, Alice and Bob can get correlated measurements in a slow fading channel. However, in vehicular communication, this is not the case because vehicles can move fast and the coherence time can be as short as a few hundred μs. In a 20 MHz channel spacing IEEE 802.11 OFDM system, a packet with a maximum rate and minimum length results in an over-the-air time of 34 μs, which cannot be considered negligible compared to the coherence time.

There has been research effort applying key generation in vehicular communication [49], [95], [96]. An RSS-based key generation system has been implemented using off-the-shelf IEEE 802.11 radios [49]. RSS measurements are found to be swamped in the high noise level. A weighted sliding window smoothing algorithm is adopted, where Alice and Bob work cooperatively to maximize the correlation coefficient of the quantized bit sequences. Level crossing is used in their system but is improved by dynamic parameter adjusting in order to adapt to the dramatic channel changes. They achieve a secure system with a bit rate around 5 b/s.

A novel distance reciprocity-based key generation is designed in [96]. While the distance may be measured using infrared and ultrasound localization systems, a wireless radios system equipped with TelosB motes is used as an example. The distance is measured through the long time-averaged RSS values therefore the fluctuations due to fading and shadowing are eliminated. As the distance does not change much in a short time interval, the legitimate users can agree on the same keys.

VIII. CONCLUSION AND SUGGESTIONS FOR FUTURE RESEARCH

Key generation from the randomness of wireless communication channels is a promising technique to share cryptographic keys securely between legitimate users. It is relatively easy to implement using off-the-shelf wireless NICs and can achieve information-theoretic security. This paper focused on the techniques of key generation systems, specifically, we reviewed the key generation principles, metrics and procedure. We also discussed methods to optimize the key generation performance. Different application scenarios were surveyed in order to clarify the features and challenges of each environment.

There are still open questions to be resolved in order to make key generation more robust [18], [42]. Some future research scopes are summarized below.

- Key generation in static environments. Although researchers have tried to introduce randomness into static channels by employing random beamforming [97], virtual channels [98] and jamming [85], [99], these methods are not generic as they either require multi-antenna [97], [98], aid from other nodes [85] or OFDM modulation [99]. The ability to operate in a static environment will be essential for the application of key generation systems.
- Group key generation. There are already some group key generation protocols [23], [26], [47], [100]–[102], but most key generation systems can still only extract keys in pairs. Group key generation has a wide range of applications. For example, in ad hoc networks, all the users will have to exchange secured information and the network is quite dynamic as there may be many users frequently joining and leaving.
- Attacks against key generation systems. This research topic currently receives limited research input. Key generation is vulnerable both to passive eavesdropping [44], [103] and active attacks [104], [105], or combined [106]. Research into how we can subvert or defend against such attacks is essential if we are to construct robust and secure key generation systems.

REFERENCES

[1] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*, Y. Xiao, X. Shen, and D.-Z. Du, Eds. New York, NY, USA: Springer, 2007, pp. 103–135.

[2] L. Chen, J. Ji, and Z. Zhang, Eds., *Wireless Network Security : Theories and Applications*. Springer, 2013.

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[4] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2013.

[5] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[6] S. Mathur *et al.*, "Exploiting the physical layer for enhanced security [Security and Privacy in Emerging Wireless Networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 63–70, Oct. 2010.

[7] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[8] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[9] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[10] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proc. IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.

[11] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[12] G. S. Vernam, "Secret signaling system," U.S. Patent 1 310 719, Jul. 12, 1919.

[13] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[14] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[15] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[16] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.
[17] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Netw.*, vol. 21, no. 6, pp. 1835–1846, Aug. 2015.
[18] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.
[19] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.
[20] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, San Francisco, CA, USA, Sep. 2008, pp. 128–139.
[21] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Beijing, China, Sep. 2009, pp. 321–332.
[22] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. 29th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, San Diego, CA, USA, Mar. 2010, pp. 1–9.
[23] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. 31st IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Orlando, FL, USA, Mar. 2012, pp. 927–935.
[24] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.
[25] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776, Dec. 2014.
[26] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, Dec. 2014.
[27] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1779–1790, Sep. 2013.
[28] L. Yao, S. T. Ali, V. Sivaraman, and D. Ostry, "Decorrelating secret bit extraction via channel hopping in body area networks," in *Proc. 23rd IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Sydney, NSW, Australia, Sep. 2012, pp. 1454–1459.
[29] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "ProxiMate: Proximity-based secure pairing using ambient wireless signals," in *Proc. 9th Int. Conf. Mobile Syst., Appl., Services (MobiSys)*, Washington, DC, USA, Jul. 2011, pp. 211–224.
[30] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 3048–3056.
[31] W. Xi *et al.*, "KEEP: Fast secret key extraction protocol for D2D communication," in *Proc. 22nd IEEE Int. Symp. Quality Service (IWQoS)*, Hong Kong, May 2014, pp. 350–359.
[32] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.
[33] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.
[34] B. T. Quist and M. A. Jensen, "Maximizing the secret key rate for informed radios under different channel conditions," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 5146–5153, Oct. 2013.
[35] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels," in *Proc. IEEE GLOBECOM Workshop Trusted Commun. Phys. Layer Secur. (TCPLS)*, Atlanta, GA, USA, Dec. 2013, pp. 1245–1250.
[36] B. T. Quist and M. A. Jensen, "Maximization of the channel-based key establishment rate in MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5565–5573, Oct. 2015.
[37] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[38] S. T.-B. Hamida, J.-B. Pierrot, and C. Castelluccia, "Empirical analysis of UWB channel characteristics for secret key generation in indoor environments," in *Proc. 21st IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Instanbul, Turkey, Sep. 2010, pp. 1984–1989.
[39] F. Marino, E. Paolini, and M. Chiani, "Secret key extraction from a UWB channel: Analysis in a real environment," in *Proc. IEEE Int. Conf. Ultra-WideBand (ICUWB)*, Paris, France, Sep. 2014, pp. 80–85.
[40] M. G. Madiseh, S. He, M. L. McGuire, S. W. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dresden, Germany, Jun. 2009, pp. 1–5.
[41] C. T. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction," in *Proc. Workshop Wireless Commun. Secur. Phys. Layer*, Coimbra, Portugal, Jul. 2015.
[42] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.
[43] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 200–204.
[44] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proc. 4th Eur. Workshop Syst. Secur.*, Salzburg, Austria, Apr. 2011, pp. 8:1–8:6.
[45] X. He, H. Dai, Y. Huang, D. Wang, W. Shen, and P. Ning, "The security of link signature: A view from channel models," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, San Francisco, CA, USA, Oct. 2014, pp. 103–108.
[46] A. L. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-22, Apr. 2010.
[47] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. 30th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1422–1430.
[48] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.
[49] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Extracting secret key from wireless link dynamics in vehicular environments," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 2283–2291.
[50] S. N. Premnath *et al.*, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.
[51] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.
[52] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52–55, Feb. 2000.
[53] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Las Vegas, NV, USA, Apr. 2008, pp. 3013–3016.
[54] Y. El Hajj Shehadeh and D. Hogrefe, "An optimal guard-intervals based mechanism for key generation from multipath wireless channels," in *Proc. 4th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Paris, France, Feb. 2011, pp. 1–5.
[55] Y. El Hajj Shehadeh, O. Alfandi, K. Tout, and D. Hogrefe, "Intelligent mechanisms for key generation from multipath wireless channels," in *Proc. Wireless Telecommun. Symp. (WTS)*, New York, NY, USA, Apr. 2011, pp. 1–6.
[56] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.
[57] M. G. Madiseh, M. L. McGuire, S. S. Neville, L. Cai, and M. Horie, "Secret key generation and agreement in UWB communication channels," in *Proc. IEEE GLOBECOM*, New Orleans, LO, USA, Nov./Dec. 2008, pp. 1–5.

[58] S. T.-B. Hamida, J.-B. Pierrot, and C. Castelluccia, "An adaptive quantization algorithm for secret key generation using radio channel measurements," in *Proc. 3rd Int. Conf. New Technol., Mobility Secur. (NTMS)*, Cairo, Egypt, Dec. 2009, pp. 1–5.

[59] J. Huang and T. Jiang, "Dynamic secret key generation exploiting ultra-wideband wireless channel characteristics," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, New Orleans, LA, USA, Mar. 2015, pp. 1701–1706.

[60] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications With MATLAB*. New York, NY, USA: Wiley, 2010.

[61] X. Wang, P. Ho, and Y. Wu, "Robust channel estimation and ISI cancellation for OFDM systems with suppressed features," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 5, pp. 963–972, May 2005.

[62] Y. Li, L. J. Cimini, and N. R. Sollenberger, "Robust channel estimation for OFDM systems with rapid dispersive fading channels," *IEEE Trans. Commun.*, vol. 46, no. 7, pp. 902–915, Jul. 1998.

[63] J. Cai, X. Shen, and J. W. Mark, "Robust channel estimation for OFDM wireless communication systems—An H_∞ approach," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 2060–2071, Nov. 2004.

[64] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Secure key generation from OFDM subcarriers' channel responses," in *Proc. IEEE GLOBECOM Workshop Trusted Commun. Phys. Layer Secur. (TCPLS)*, Austin, TX, USA, Dec. 2014, pp. 1302–1307.

[65] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual OFDM subcarrier's channel response," in *Proc. IEEE GLOBECOM Workshop Trusted Commun. Phys. Layer Secur. (TCPLS)*, San Diego, CA, USA, Dec. 2015.

[66] M. F. Haroun and T. A. Gulliver, "Secret key generation using chaotic signals over frequency selective fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1764–1775, Aug. 2015.

[67] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11n traces with channel state information," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 1, p. 53, Jan. 2011.

[68] *Ettus Research*. [Online]. Available: http://www.ettus.com, accessed Jan. 27, 2016.

[69] *WARP Project*. [Online]. Available: http://warpproject.org, accessed Jan. 27, 2016.

[70] R. Guillaume, F. Winzer, and A. Czylwik, "Bringing PHY-based key generation into the field: An evaluation for practical scenarios," in *Proc. 82nd IEEE Veh. Technol. Conf. (VTC Fall)*, Boston, MA, USA, Sep. 2015.

[71] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[72] J. Bardwell. *You Believe You Understand What You Think I Said—The Truth About 802.11 Signal and Noise Metrics*. [Online]. Available: http://www.n-cg.net/ncgpdf/WiFi_SignalValues.pdf, accessed Jan. 27, 2016.

[73] *MICAz Wireless Measurement System*. [Online]. Available: http://www.memsic.com/userfiles/files/Datasheets/WSN/micaz_datasheet-t.pdf, accessed Jan. 27, 2016.

[74] *Crossbow TelosB Mote Platform*. [Online]. Available: http://www.willow.co.uk/TelosB_Datasheet.pdf, accessed Jan. 27, 2016.

[75] S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, and R. Ricci, "Secret key extraction using Bluetooth wireless signal strength measurements," in *Proc. 11th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Singapore, Jun./Jul. 2014, pp. 293–301.

[76] K. Chen, B. B. Natarajan, and S. Shattil, "Secret key generation rate with power allocation in relay-based LTE-A networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2424–2434, Nov. 2015.

[77] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, Alexandria, Egypt, Oct. 2007, pp. 401–410.

[78] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "An effective key generation system using improved channel reciprocity," in *Proc. 40th IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Brisbane, QLD, Australia, Apr. 2015, pp. 1727–1731.

[79] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1842–1852, Sep. 2013.

[80] R. Guillaume, A. Mueller, C. T. Zenger, C. Paar, and A. Czylwik, "Fair comparison and evaluation of quantization schemes for PHY-based key generation," in *Proc. 18th Int. OFDM Workshop (InOWo)*, Essen, Germany, Aug. 2014, pp. 1–5.

[81] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. Workshop Theory Appl. Cryptograph. Tech. Adv. Cryptol. (EUROCRYPT)*, 1994, pp. 410–423.

[82] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[83] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[84] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.

[85] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "SmokeGrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1731–1745, Nov. 2013.

[86] J. Zhang, S. K. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, San Diego, CA, USA, Mar. 2010, pp. 1–5.

[87] A. Ambekar, M. Hassan, and H. D. Schotten, "Improving channel reciprocity for effective key management systems," in *Proc. Int. Symp. Signals, Syst., Electron. (ISSSE)*, Potsdam, Germany, Oct. 2012, pp. 1–4.

[88] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[89] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[90] C. D. T. Thai, J. Lee, C. Cheng, and T. Q. S. Quek, "Physical-layer secret key generation with untrusted relays," in *Proc. IEEE GLOBECOM Workshop Trusted Commun. Phys. Layer Secur. (TCPLS)*, Austin, TX, USA, Dec. 2014, pp. 1385–1390.

[91] N. Wang, N. Zhang, and T. A. Gulliver, "Cooperative key agreement for wireless networking: Key rates and practical protocol design," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 272–284, Feb. 2014.

[92] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. M. Leung, "Recent advances in industrial wireless sensor networks toward efficient management in IoT," *IEEE Access*, vol. 3, pp. 622–637, Jun. 2015.

[93] C. T. Zenger, M.-J. Chur, J.-F. Posielek, C. Paar, and G. Wunder, "A novel key generating architecture for wireless low-resource devices," in *Proc. Int. Workshop Secure Internet Things (SIoT)*, Wroclaw, Poland, Sep. 2014, pp. 26–34.

[94] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1635–1657, Aug. 2014.

[95] B. Zan, M. Gruteser, and F. Hu, "Key agreement algorithms for vehicular communication networks based on reciprocity and diversity theorems," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 4020–4027, Oct. 2013.

[96] O. Gungor, F. Chen, and C. E. Koksal, "Secret key generation via localization and mobility," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2214–2230, Jun. 2015.

[97] M. G. Madiseh, S. W. Neville, and M. L. McGuire, "Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1278–1287, Aug. 2012.

[98] P. Huang and X. Wang, "Fast secret key generation in static wireless networks: A virtual channel approach," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 2292–2300.

[99] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. 30th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1125–1133.

[100] Y. Wei, C. Zhu, and J. Ni, "Group secret key generation algorithm from wireless signal strength," in *Proc. 6th Int. Conf. Internet Comput. Sci. Eng. (ICICSE)*, Henan, China, Apr. 2012, pp. 239–245.

[101] C. Ye and A. Reznik, "Group secret key generation algorithms," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, Jun. 2007, pp. 2596–2600.
[102] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Secret group key generation in physical layer for mesh topology," in *Proc. IEEE GLOBECOM*, San Diego, CA, USA, Dec. 2015.
[103] D. Steinmetzer, M. Schulz, and M. Hollick, "Lockpicking physical layer key exchange: Weak adversary models invite the thief," in *Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, New York, NY, USA, Jun. 2015, pp. 1–11.
[104] H. Zhou, L. M. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 476–488, Mar. 2014.
[105] R. Jin and K. Zeng, "Physical layer key agreement under signal injection attacks," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Florence, Italy, Sep. 2015, pp. 254–262.
[106] M. Clark, "Robust wireless channel based secret key extraction," in *Proc. Military Commun. Conf. (MILCOM)*, Orlando, FL, USA, Oct./Nov. 2012, pp. 1–6.

JUNQING ZHANG received the B.Eng. and M.Eng. degrees in electrical engineering from Tianjin University, China, in 2009 and 2012, respectively. He is currently pursuing the Ph.D. degree in electronics and electrical engineering with Queen's University Belfast, U.K. His research interests include physical layer security, cryptography, and OFDM.

TRUNG Q. DUONG (S'05–M'12–SM'13) received the Ph.D. degree in telecommunications systems from the Blekinge Institute of Technology, Sweden, in 2012. Since 2013, he has been with Queen's University Belfast, U.K., as a Lecturer (Assistant Professor). He has authored or co-authored 170 technical papers in scientific journals and presented at international conferences. His current research interests include cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, millimeter-waves communications, and localization for radios and networks.

Dr. Duong received the best paper award at the IEEE Vehicular Technology Conference in 2013, and the IEEE International Conference on Communications in 2014. He is a recipient of the Royal Academy of Engineering Research Fellowship. He currently serves as an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE COMMUNICATIONS LETTERS, *IET Communications*, *Wiley Transactions on Emerging Telecommunications Technologies*, and *Electronics Letters*. He has also served as the Guest Editor of the special issue on some major journals, including the IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, *IET Communications*, the *IEEE Wireless Communications Magazine*, the *IEEE Communications Magazine*, the *EURASIP Journal on Wireless Communications and Networking*, and the *EURASIP Journal on Advances Signal Processing*.

ALAN MARSHALL (M'88–SM'00) holds the Chair in Communications Networks with the University of Liverpool, where he is the Director of the Advanced Networks Group. He has spent over 24 years with the Telecommunications and Defense Industries. He has been a Visiting Professor of Network Security with the University of Nice/CNRS, France, and an Adjunct Professor for Research with Sunway University Malaysia. He has formed a successful spin-out company, Traffic Observation & Management Ltd., specializing in intrusion detection and prevention for wireless networks. He has authored over 200 scientific papers and holds a number of joint patents in the areas of communications and network security. His research interests include network architectures and protocols, mobile and wireless networks, network security, high-speed packet switching, quality of service and experience (QoS/QoE) architectures, and distributed haptics. He is a fellow of the IET.

ROGER WOODS (M'95–SM'01) received the B.Sc. (Hons.) degree in electrical and electronic engineering and the Ph.D. degree from Queen's University Belfast, in 1985 and 1990, respectively. He has co-founded a spin-off company, Analytics Engines Ltd., which looks to exploit a lot of the programmable systems research. He is currently a Full Professor with Queen's University Belfast and has created and leads the Programmable Systems Laboratory. He holds four patents, and has authored over 170 papers. His research interests are in heterogeneous programmable systems and system level design tools for data, signal and image processing, and telecommunications. He is a member of the IEEE Signal Processing and Industrial Electronics Societies and is on the Advisory Board of the IEEE SPS Technical Committee on the Design and Implementation of Signal Processing Systems. He is on the Editorial Board of the *ACM Transactions on Reconfigurable Technology and Systems*, the *Journal of VLSI Signal Processing Systems*, and the *IET Proceedings on Computer and Digital Techniques*. He acted as the General Chair of the 2014 Asilomar IEEE Conference on Signals, Systems, and Computers, and is on the program committees of a number of IEEE conferences.