A Channel Perceiving Attack and the Countermeasure on Long-Range IoT Physical Layer Key Generation

Lu Yang[a,*], Yansong Gao[b], Junqing Zhang[c], Seyit Camtepe[b], Dhammika Jayalath[a]

[a] *Science and Engineering Faculty, Queensland University of Technology, Brisbane, Australia*
[b] *Data61, CSIRO, Sydney, Australia*
[c] *Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom*

Abstract

Physical layer key generation is a lightweight technique to generate secret keys from wireless channels for resource-constrained Internet of things (IoT) applications. The security of the key generation relies on spatial decorrelation, which assumes that eavesdroppers observe uncorrelated channel measurements when they are located over a half-wavelength away from legitimate users. Unfortunately, no experimental validation exists for communications environments with both large-scale and small-scale fading effects. Furthermore, while the current key generation work mainly focuses on short-range communications techniques such as WiFi and ZigBee, the exploration with long-range communications, e.g., LoRa, is somewhat limited. This paper presents a long-range key generation testbed and reveals a new attack scenario that perceives and utilizes large-scale fading effects in key generation channels, by using multiple eavesdroppers circularly around a legitimate user. We formalized such an attack and validated it through extensive experiments conducted in indoor and outdoor environments. It is corroborated that the attack reduces secret key capacity when large-scale fading is predominant. We further investigated potential defenses by proposing a conditional entropy and high-pass filter-based countermeasure to estimate and eliminate large-scale fading components. The experimental results demonstrated that the countermeasure significantly improved the key generation's security when both large-scale and small-scale fading existed. The keys generated by legitimate users have a desirable low key disagreement rate (KDR) and are validated by the NIST randomness tests. In contrast, eavesdroppers' average KDR is increased from 0.25 to 0.49.

Keywords: Large-scale fading, long-range IoT, physical layer key generation, security defense, secret key capacity

1. Introduction

Internet of things (IoT) has triggered extensive exciting applications, including health monitoring, environmental sensing, and industrial control [1]. Information security of IoT networks is essential as the information exchanged may be essential, private, and sensitive [2, 3]. It is usually achieved by symmetric encryption algorithms and key distribution schemes. The former, e.g., advanced encryption standard (AES), is used to protect the data using a symmetric key. The latter is currently handled by the conventional public-key cryptography (PKC), such as the elliptic-curve Diffie-Hellman (ECDH) key exchange. PKC schemes rely on complicated mathematical problems, such as discrete logarithms. Hence, they are computationally expensive, which results in high power consumption and may not be suitable for resource-constrained IoT devices [4]. Furthermore, managing the PKC in decentralized IoT networks is difficult as the public key infrastructure may not always be available [5, 6]. Finally, PKC schemes will become vulnerable to emerging quantum computers because they are not scalable [7].

In order to address this challenge, particularly for low-cost IoT devices, an alternative technique named *key generation from wireless channels*, which has attracted extensive research interests [4, 8, 9, 10, 11]. This technique exploits the randomness from the shared wireless channel between a pair of users to generate secret keys; hence, it is information-theoretically secure [12, 13]. In addition, it is not complicated and consumes much less power than PKC schemes, which is suitable for low-cost IoT devices. For example, Zenger *et al.* implemented a key generation protocol on an 8-bit Intel MCS-51 micro-controller, and showed the energy cost to generate a 128-bit secret key is 98 times less than that of the ECDH key exchange [14].

Key generation mainly exploits multipath [15], and employs the randomness in temporal [16, 17], frequency [18, 19, 20], and spatial domains [20, 21, 22]. Local induced randomness enhances the key generation performance in a multipath limited environment [23, 24]. The security level of the key generation against eavesdropping relies on spatial decorrelation. In a multipath-rich environment, when an eavesdropper is more than a half-wavelength away

*Corresponding author
Email addresses: l41.yang@hdr.qut.edu.au (Lu Yang), garrison.gao@data61.csiro.au (Yansong Gao), junqing.zhang@liverpool.ac.uk (Junqing Zhang), seyit.camtepe@data61.csiro.au (Seyit Camtepe), dhammika.jayalath@qut.edu.au (Dhammika Jayalath)

from legitimate users, the eavesdropper experiences uncorrelated channels, hence the eavesdropper cannot infer correct keys. This assumption is determined from the Bessel function developed for a sum of multipath signals [25]. The core interest is to validate the spatial decorrelation assumption in practice [26, 27, 28]. Edman *et al.* designed a ZigBee-based testbed and experimentally demonstrated that the eavesdropper's capability of secret key inference reduces as the distance between an eavesdropper to legitimate users increases [26]; they also found that the required distance for securing at least 50% secret key information is far more than a half-wavelength. Zhang *et al.* constructed a WiFi-based testbed and also carried out extensive measurements in different environments, including an anechoic chamber (no multipath), a reverberation chamber (very rich multipath), and an indoor office (normal multipath) [27]. They found that key generation security significantly relies on the multipath levels of the environments. In particular, the secure distance should be much larger than a half-wavelength in an environment where multipath is limited. However, none of them provided corresponding countermeasures against eavesdropping. In addition, all the above experimental validation was performed with short-range communications; *the spatial decorrelation assumption is not clear in long-range communications when large-scale fading is present.*

In practice, eavesdroppers may seek collusion to reveal more information in key generation. Thai *et al.* investigated and proposed a multi-antenna-based scheme that achieves high secret key rates over colluding eavesdroppers and non-trusted relays [29]. Waqas *et al.* investigated secret key generation as eavesdroppers colluded in a social network and designed an algorithm for high secret key generation rates [30, 31]. These works rely on multiple antennas or relays, which may not apply to the networks deployed with low-cost IoT devices.

IoT can be categorized into wireless local area networks (WLAN), wireless personal area networks (WPAN) as well as low-power wide-area networks (LPWAN). WLAN and WPAN are short-range communications systems, such as WiFi and ZigBee, respectively. Key generation has been mainly applied with them so far, such as WiFi [27, 32], ZigBee [33], and Bluetooth [34]. There have been extensive measurements campaigns to demonstrate the feasibility of key generation with these communications technologies.

LPWAN is an important element of IoT with representative technologies such as LoRa and Narrowband Internet of Things (NB-IoT) and has become the key enabler of many transformative IoT applications [35, 36]. In comparison with WLAN and WPAN, key generation applied with LPWAN is rather limited, with some preliminary experimental explorations reported in [37, 38, 39, 40, 41] and simulation work on large-scale fading for key generation [42]. Ruotsalainen *et al.* investigated the effects of LoRa setup on key generation performance [37, 41]. Zhang *et al.* designed a differential value-based key generation protocol for LoRa and validated the performance in both indoor and urban environments [39]. Xu *et al.* also proposed a LoRa-based protocol and carried out extensive experiments [40]. However, a systematic investigation of eavesdropping attacks on long-range key generation is *currently missing* and urgently required for security validation.

For long-range wireless communications, signals traveling longer distances have more significant and predictable attenuation due to large-scale fading effects. The predictable attenuation leads to predictable received signal characteristics that can compromise the long-range key generation. Furthermore, there will be barely non-hostile key generation environments as the LPWAN is often deployed under insufficient surveillance. For example, networks deployed on highways, farmlands, and national parks face various threats to reduce the secret key capacity, constrain the key generation rate, and compromise the key.

The above research challenges motivated us to reveal and investigate an unstudied key generation attack scenario in long-range communications and devise a secure long-range key generation protocol under the impact of large-scale fading. The novelty of the proposed attack scenario and the countermeasure are justified as follows.

- Large-scale fading has not been known to leak secret keys in key generation, but it is naturally presented in long-range communications.
- The spatial decorrelation assumption was not practically validated in the presence of large-scale fading variation, though it is the ground for the key generation security.
- No prior work exists that constructively explores the high-pass filter implementation to improve the key generation security.

Our contributions are listed as follows.

1. A long-range communications testbed is designed, and extensive experiments are carried out to investigate the impact of large-scale fading on the key generation.
2. *A new channel-perceiving attack scenario* is revealed and guided by our formalization to validate the spatial decorrelation assumption. The attack perceives large-scale fading effects in key generation channels, by using multiple eavesdroppers circularly around a legitimate user. The experimental results demonstrated that the colluding eavesdroppers can infer a higher portion of secret keys utilizing large-scale fading variation. We also demonstrated that the secret key inference capability of the revealed attack can be boosted by the signal pre-processing techniques that are often adopted in practice to enhance the key generation.
3. *A conditional entropy and high-pass filtering countermeasure* is proposed to mitigate the effect of this newly revealed attack. In particular, key generation

users can estimate large-scale fading associated low-frequency components using their channel observations and remove them without losing much randomness. The results showed that the key leakage was mitigated as colluding eavesdroppers' KDR increased significantly. The NIST randomness tests validated the randomness of the large-scale fading filtered key bits.

The rest of the paper is organized as follows. Section 2 introduces the preliminary knowledge of key generation and the model used in the experiments. Section 3 presents the new colluding-eavesdropping attack and formalizes its large-scale fading estimation and secret key inference capabilities. Section 4 describes the experimental setup and analytical metrics. Section 5 presents the experimental analysis. Section 6 proposes the countermeasure against the revealed attack. Finally, Section 7 concludes the paper.

2. Preliminary

2.1. Key Generation Protocol

The wireless channel between two users is the ideal source of randomness to generate secret keys for cryptographic applications [11, 13]. Suppose Alice and Bob want to generate a shared key using the randomness of the wireless channel. Due to channel reciprocity, they measure and analyze identical channel characteristics by sending and receiving known data packets. These measurements can then be transferred to binary sequences for encryption purposes. Detailed protocol generally incorporates the following steps.

1. *Channel Probing:* Bi-directional measurements are taken between key generation users. The measured channel characteristics are analyzed and stored in sequences. The probing packets do not have to carry useful messages, but it is important to have similar packet sizes to avoid power offset in transmission.
2. *Signal Pre-Processing:* The step is optional in a traditional key generation process but widely applied to mitigate the discrepancies brought by hardware impairment and channel noise. Signal pre-processing techniques can be classified into filtering and interpolation, where the first is to eliminate mismatches and the second is to fill in missing values. An advantageous technique should greatly improve measurement correlation without being high-cost and introducing security threats.
3. *Quantization:* Each channel characteristic value of a sequence is mapped to a binary bit.
4. *Information Reconciliation:* Although the channel characteristics are highly correlated with users, slight mismatches are unavoidable in practice. A single bit difference can fail to decrypt messages. Therefore, error detection protocol-based approaches (EDPA) and error correction code-based approaches (ECCA) are used to cope with the bit difference after quantization. The resulted bit strings are perfectly matched after the reconciliation.
5. *Privacy Amplification:* Users need to exchange error-correcting messages in public channels in the information reconciliation step, and the messages can reveal some bit information. Therefore, it is important to discard the partial information. This is often developed using hash functions in practice.

Among the key generation steps, channel probing is the only step to introduce randomness, and it is sensitive to large-scale fading variations. The broadcasting nature of wireless communications makes channel probing most vulnerable to eavesdropping, where the other steps are mostly encrypted and processed offline. Hence our experiments focused on channel probing and signal pre-processing as both measure raw channel characteristics.

2.2. User and Threat Model

The user model consists of two end devices that separated far enough to introduce large-scale fading. The devices communicate directly with predetermined long-range techniques (e.g., LoRa). One end device serves as a stationary base station, and the other is either a mobile node or a stationary node depending on the large-scale fading variation in experiments. The communication link is secure, and no active adversary to disrupt or jam at all stages of signal transmission.

Following the traditional threat model in key generation research, we assume eavesdroppers listen to all users' communications. Hardware discrepancies are negligible. There is no restricted key generation protocol information to access (e.g., signal pre-processing techniques). There is also no restriction on communication protocol information; therefore, eavesdroppers should know all signal sources, types, and sequences. Further, eavesdroppers can exchange their measurements in and out of listening, and users cannot detect the communication. Last, eavesdroppers can move freely but never into a half-carrier-wavelength range of legitimate users.

2.3. Large-Scale Fading Model

Channel effect is a superposition of small-scale and large-scale fading [25]. Small-scale fading is caused by the constructive and destructive interference of signals due to reflection, diffraction, and scattering. It is unpredictable as it can be affected by even a very slight movement of the device or the environment. Hence, it introduces randomness to received signal characteristics over a short time and distance.

In contrast, large-scale fading introduces a more significant attenuation to the received signal over a long distance, which is consisted of path loss and shadow fading. Path loss describes the signal attenuation along with the distance while shadowing is caused by the blocking of large

obstacles such as buildings. From a far-field transmitter to a receiver, the path loss effect in the linear scale can be expressed as [25]

$$P_{r,lin} = P_{t,lin} G_{lin} \left(\frac{d_0}{d}\right)^{\gamma} \tag{1}$$

where $P_{t,lin}$ is the transmission power, G_{lin} denotes the combined system gains, γ is the path loss exponent, d_0 is the reference distance, and d is the distance from the transmitter to the receiver.

For the simplification of notation, the received power is usually represented in the logarithm scale. The overall received power affected by both the path loss and shadow fading can be given as [25]

$$P_r = P_t + G - \underbrace{10\gamma \log_{10}\left(\frac{d}{d_0}\right)}_{\text{path loss}} - \underbrace{\chi}_{\text{shadowing}} \tag{2}$$

where P_t and G are the transmission power and system gains in the logarithm scale, and χ is a log-normal distributed shadowing component with a zero mean ($\mu_\chi = 0$ dB).

As most of the existing key generation works focus on short-range communications such as WiFi, small-scale fading has been exploited as their random sources [15, 18, 27]. Following the initial LoRa-based work in [37, 38, 39, 40, 41], this paper will take a step further to investigate the key generation performance when there are large-scale fading and small-scale fading effects. In particular, its security against a large-scale fading resulted colluding-eavesdropping attack will be examined.

3. A New Large-Scale Fading Resulted Colluding-Eavesdropping Attack

Two legitimate users, namely Alice and Bob, wish to generate the same key from the randomness of their shared wireless channel. This will require channel probing, which involves bidirectional wireless transmissions between Alice and Bob. They will alternately transmit probing signals. Thanks to the channel reciprocity property, when the probing delay is much smaller than the coherence time, $h_{AB} = h_{BA}$ will hold, where h_{uv} is the channel effect between users u and v. Hence, both users will obtain highly correlated received signal characteristics that can be exploited to generate secret keys. We used the received signal strength indicator (RSSI), which is readily accessible for LPWAN devices. Far-field communications are assumed when Alice and Bob's distance d is much larger than the carrier wavelength λ. LPWAN technologies like LoRa and NB-IoT are designed for long-range communications; thus, it is reasonable to assume $d \gg \lambda$.

When Alice and Bob are carrying out channel probing, a group of eavesdroppers can also receive all the transmissions due to the broadcast nature of wireless communications. This work considers such an attack as a colluding-eavesdropping attack, which is portrayed in Fig. 1. We

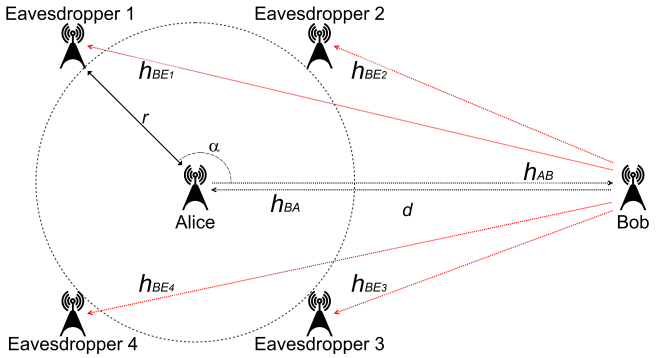

Fig. 1. A key generation setup with the large-scale fading resulted colluding-eavesdropping attack; four eavesdroppers are used for illustration.

consider M eavesdroppers uniformly and circularly distributed around Alice at a distance of r, where r is larger than a half-carrier-wavelength. The antenna gains of Alice, Bob, and the eavesdroppers are identical. The eavesdroppers passively receive the probing signals from Bob and collude to deduce the received power at Alice. For the m-th Eve, her distance to Bob can be given as

$$d_{B-E_m} = \sqrt{d^2 + r^2 - 2dr\cos\left(\alpha + \frac{2\pi(m-1)}{M}\right)} \tag{3}$$

where α is the angle between the path of Alice and Bob and the path of Alice and the first eavesdropper. If the power resulted from path loss at the m-th Eve is $P_{r,lin}^{E_m}$, the average power can be calculated as

$$\begin{aligned}\overline{P}_{r,lin}^{E} &= \frac{1}{M}\sum_{m=1}^{M} P_{r,lin}^{E_m} \\ &= \frac{1}{M}\sum_{m=1}^{M} P_{t,lin} G_{lin}\left(\frac{d_0}{d_{B-E_m}}\right)^{\gamma}\end{aligned} \tag{4}$$

As eavesdroppers aim to obtain accurate observations, they are usually not far from legitimate users, i.e., r is small. Hence, $d \gg r$ reasonably holds in LPWAN, and then $d_{B-E_m} \approx d$. We have

$$\overline{P}_{r,lin}^{E} \approx P_{t,lin} G_{lin}\left(\frac{d_0}{d}\right)^{\gamma} \tag{5}$$

The averaged received power affected by both the path loss and shadow fading in the logarithm scale can be given as

$$\overline{P_r}^{E} \approx P_t + G - 10\gamma \log_{10}\left(\frac{d}{d_0}\right) - \overline{\chi}_E \tag{6}$$

where $\overline{\chi}_E$ denotes the average shadowing.

Regarding the probing signals sent from Bob to Alice, the RSSI of Alice is denoted by P_r^A and follows the same form as (2). According to (2) and (6), the difference between the estimated power via colluding-eavesdropping and the power resulted from large-scale fading at Alice can

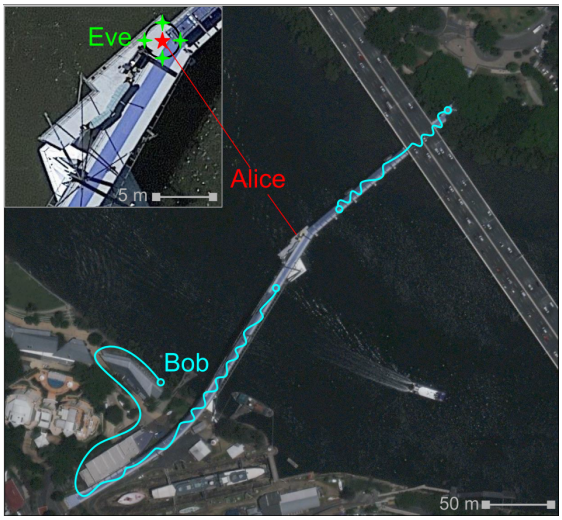

Fig. 2. Outdoor experimental environment and the trajectory of Bob.

Table 1. LoRa Configuration

Carrier Frequency	Bandwidth	Transmission Power	Spreading Factor	Coding Rate
915 MHz	500 kHz	17 dBm	7	4/5

be given as

$$\overline{P_r}^E - P_r^A = \chi - \overline{\chi}_E \tag{7}$$

The large-scale fading estimation is also affected by small-scale fading. According to the central limit theorem, a large M can minimize the small-scale fading introduced uncertainty. In practice, a large number of eavesdroppers can be discovered by legitimate users easily. Hence, we used a small number, only four eavesdroppers, in our experiments to demonstrate the colluding-eavesdropping attack, with reduced estimation accuracy resulted from small-scale fading.

4. Experimental Setup and Analytical Metrics

4.1. Experimental Setup

We used six Arduino Nano controlled LoRa SX1276 modules in our experiments, to act as Alice, Bob, and four eavesdroppers, respectively. Each module was equipped with an omnidirectional antenna. The LoRa configuration specifications are given in Table 1.

These six LoRa modules are placed as shown in Fig. 1. We considered four different scenarios, as detailed in Table 2. There was no large-scale fading variation in scenarios (a) and (b) as both Alice and Bob were static. In contrast, there was large-scale fading variation in scenarios (c) and (d) because Bob was moving.

Extensive experiments were conducted in both indoor and outdoor environments.

Table 2. Experimental Channel Summary

Scenario	Channel	Variation
(a)	Static channel	Noise
(b)	Moving scatterers	Small-scale fading and noise
(c)	Moving Bob	Large-scale fading, small-scale fading, and noise
(d)	Moving Bob and moving scatterers	Large-scale fading, small-scale fading, and noise

1. In the indoor environment, all the six devices were placed on the same floor of an apartment building, and there was no line-of-sight from Bob to Alice and the eavesdroppers. The indoor experiments covered all four scenarios, and we used (Ia), (Ib), (Ic), and (Id) to represent them, hence to ease the description after.
2. The setup of the outdoor environment is shown in Fig. 2. Alice and eavesdroppers were placed on a deck in the middle of a pedestrian bridge. Direct line-of-sight paths were present most of the time between Bob and Alice as well as between Bob and eavesdroppers. The outdoor experiments involved scenarios (b) and (d) as we were not able to control the behavior of scatterers, e.g., pedestrian. We accordingly used (Ob) and (Od) to represent the outdoor scenarios.

For scenarios (Ic), (Id), and (Od), Bob walked randomly with an average speed of 1 m/s to introduce large-scale fading variation. We varied the distance r to 2λ, 3λ, 4λ, and 5λ for each scenario. The wavelength λ is approximately 0.33 m when the carrier frequency is 915 MHz.

For each experiment, in the n-th probing, Alice first transmits a packet with 20 ms airtime to Bob who will measure the RSSI, $P_r^B(n)$; Bob will then transmit a packet with 20 ms airtime to Alice who will measure the RSSI, $P_r^A(n)$. Fixed payloads and data rates maintain the airtime; the channel coherence time in the experiments is longer than 100 ms. The channel reciprocity can thus be ensured. Meanwhile, the m-th Eve will receive the packet from Bob and measure the RSSI, $P_r^{E_m}(n)$. Alice and Bob will keep the above channel probing process until they collect sufficient samples. For the simplification of notation, we use $X_u(n) = P_r^u(n)$ to denote a measured RSSI sample at the party u in the n-th probing, where $u = \{A, B, E_m\}$ denotes Alice, Bob, and the m-th eavesdropper, respectively. $X_{E_c}(n)$ denotes the RSSI sample estimated by the colluding-eavesdropping attack, i.e., $\overline{P_r}^E$. Alice and Bob carried out channel probing for more than three minutes and collected at least $N = 10{,}000$ RSSI samples.

4.2. Analytical Metrics

We used cross-correlation, secret key capacity, and intact key information ratio as the analytical metrics.

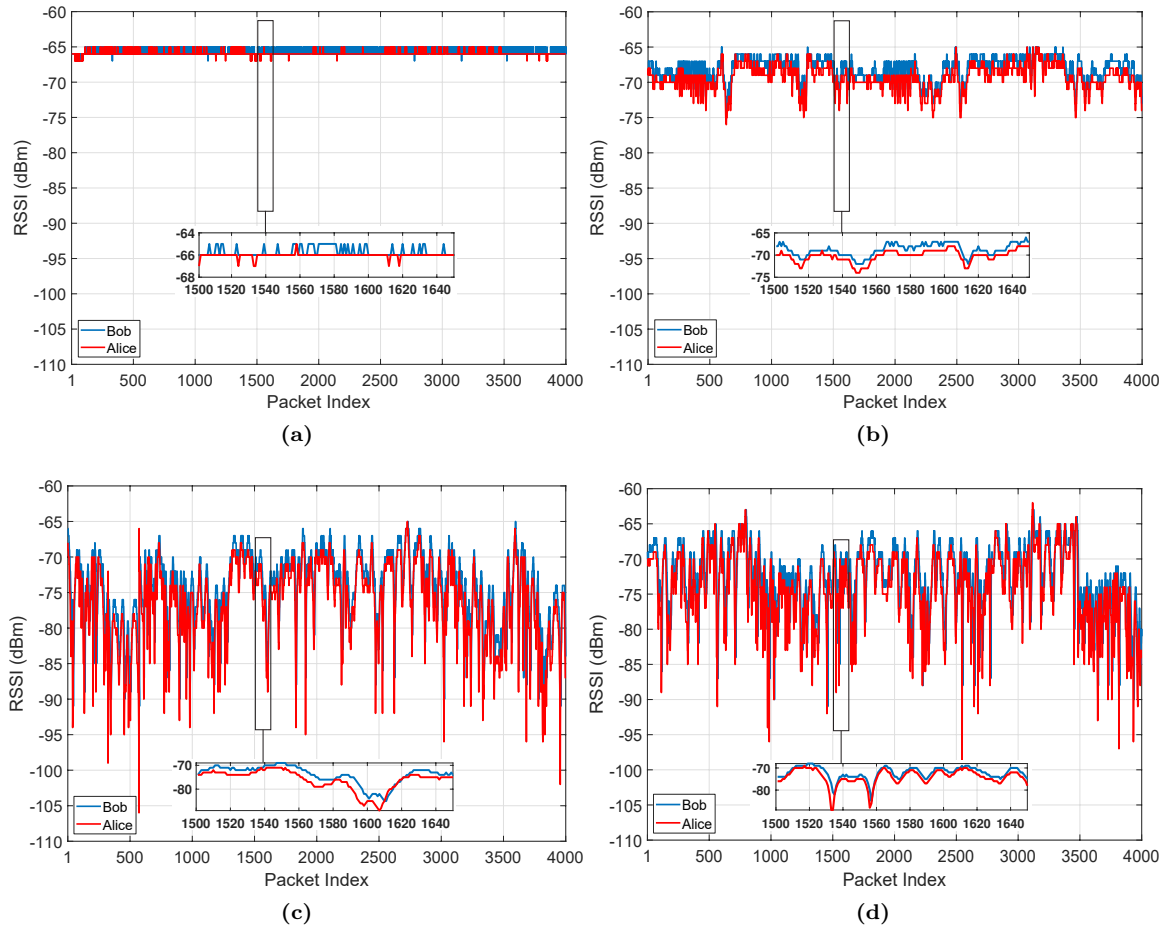

Fig. 3. RSSI sequences in indoor experiments (4000 samples in each sequence are selected for demonstration). (a) Static scenario (Ia). (b) Channel with moving scatterers (Ib). (c) Channel with moving Bob (Ic). (d) Channel with moving Bob and moving scatterers (Id).

4.2.1. Cross-Correlation

The Pearson correlation coefficient for the RSSI sequences measured by Alice and Bob and the m-th eavesdropper is defined as

$$\rho_{u,v} = \frac{\sum_{n=1}^{N}[(X_u(n)-\mu_u)(X_v(n)-\mu_v)]}{\sqrt{\sum_{n=1}^{N}(X_u(n)-\mu_u)^2}\sqrt{\sum_{n=1}^{N}(X_v(n)-\mu_v)^2}} \tag{8}$$

where $u = A$ and $v = B, E_c, E_m$, $m = 1, 2, 3, 4$. When eavesdroppers obtain correlated RSSI sequences, they can develop an accurate secret key inference.

4.2.2. Secret Key Capacity

The secret key capacity describes the maximum key generation rate [13, 43, 44]. It can be expressed as

$$C_K = \min[I(X_A;X_B), I(X_A;X_B|X_{E_m}), I(X_A;X_B|X_{E_c})] \tag{9}$$

where $I(X;Y)$ denotes the mutual information between X and Y and can be given as

$$I(X;Y) = H(X) - H(X|Y) \tag{10}$$

$$= -\sum_{x\in X} p(x)\log_2 p(x) + \sum_{y\in Y}\sum_{x\in X} p(x,y)\log_2 p(x|y) \tag{11}$$

$p[X_u(n)]$ was calculated according to the observing frequency of $X_u(n)$. Before calculating the mutual information, we normalized RSSI samples to remove DC offset.

In our analysis, C_K is upper-bounded by the minimum among the mutual information of Alice and Bob, the conditional mutual information given by an eavesdropper, and the conditional mutual information given by the colluding-eavesdropping attack. A higher C_K stands for more key bits can be generated from an RSSI sequence.

4.2.3. Intact Key Information Ratio

The intact key information ratio is defined as

$$R_{C_K} = \frac{C_K}{I(X_A;X_B)} \tag{12}$$

The ratio determines the proportion of an RSSI sequence that is not leaked. R_{C_K} closes to one is desirable as it indicates eavesdroppers have the least information related to key generation.

5. Attack Results and Discussion

Fig. 3 shows the RSSI sequences measured by Alice and Bob in the scenarios (Ia), (Ib), (Ic), and (Id) of the indoor experiments. As can be observed from Fig. 3(a), there was no noticeable random variation at Alice and Bob, which would not be suitable for key generation. Comparing the Fig. 3(b) with Fig. 3(c) and Fig. 3(d), large-scale fading brought significant RSSI changes. This section firstly investigated the impact of large-scale fading variation on key generation through cross-correlation and secret key capacity analysis. Then, we investigated the effect of signal pre-processing on the intact key information ratio.

5.1. Cross-Correlation Analysis

Fig. 4 and Fig. 5 show the cross-correlation analysis results for indoor and outdoor experiments, respectively. The red bars are obtained by calculating the highest Pearson correlation coefficient among the four eavesdroppers and Alice. Hence, it represents the optimal capability of secret key inference developed by a single eavesdropper. The black bar is obtained by calculating the Pearson correlation coefficient between the colluding-eavesdropping attack and Alice.

In the static scenario (Ia), $|\rho_{A,B}|$ is very small, which echos the RSSI sequence shown in Fig. 3(a). This is because the signal variation is introduced by hardware thermal noise and/or interference, which are not correlated. Key generation in static scenarios will thus not be feasible.

One observation from the figures is that the colluding-eavesdropping attack in the scenarios (Ic) and (Id) produces higher coefficients than any single eavesdropper. Bob was stationary in the scenarios (Ia) and (Ib), the colluding-eavesdropping attack does not outperform a single eavesdropper. Bob was mobile in the scenarios (Ic) and (Id), the colluding-eavesdropping attack obtains more channel information generated by large-scale fading to improve channel correlation with Alice. On average, the colluding-eavesdropping attack obtained an additional 15% channel information when Bob was mobile. In all the dynamic scenarios, the cross-correlation coefficients between Alice and Bob are much higher.

5.2. Secret Key Capacity Analysis

Table 3 and Table 4 present the secret key capacity analysis results for indoor and outdoor experiments, respectively. The $I(X_A; X_B)$ demonstrates the maximum obtainable C_K when there was no eavesdropping. The elements in red color denote the true secret key capacity when eavesdropping occurred.

Observing Table 3, the results can be summarized into three categories.

1. Scenario (Ia). The scenario produces the lowest value of $I(X_A; X_B)$ because only noise was available in the static scenario. Unfortunately, hardware thermal noise is independent at each device, and there is no correlation between two devices; hence, it is not suitable for key generation.
2. Scenario (Ib). There was no large-scale fading variation, hence the colluding-eavesdropping attack has no chance to reduce the secret key capacity. The resulted $I(X_A; X_B|X_{E_c})$ is not the smallest value.
3. Scenarios (Ic) and (Id). Large-scale fading changed in the scenarios (Ic) and (Id), and the large-scale fading estimation perceived these changes that introduce randomness to the key generation between Alice and Bob. Therefore, the colluding-eavesdropping attack outperformed any single eavesdropper. This is corroborated from the table as the $I(X_A; X_B|X_{E_c})$ is always the smallest for these two scenarios.

The same pattern can be observed from Table 4 corresponding to outdoor experiments.

5.3. Intact Key Information Ratio Analysis

In the indoor experiments, an average of 92.1% RSSI information was never leaked in the scenario (Ib), 79.1% in the scenario (Ic), and 73.3% in the scenario (Id). In the outdoor experiments, the value was 80.1% in the scenario (Ob) and 72.0% in the scenario (Od). For RSSI sequences with the same number of samples, the sequences generated in large-scale fading varying channels leaked more samples to the colluding-eavesdropping attack, hence fewer secret keys were generated. In practice, key generation users can develop additional channel probing to compensate for the secret key loss, but this will also increase the key generation cost.

Signal pre-processing is commonly employed in the key generation to improve channel reciprocity [45, 46, 47, 48, 49]. Most research claim that their approaches are effective in noise cancellation and improving cross-correlation of channel measurements. They help to reduce the key generation cost, which is desirable for resource-constrained IoT devices. However, applying noise cancellation in large-scale fading-based key generation may reduce the intact key information ratio. In other words, we reveal that there is a trade-off between the benefit brought by the noise cancellation and the security deduction of the key generation. The detailed analysis is shown as follows.

A moving window average (MWA) technique is investigated as it is practical and convenient to reduce noise. The MWA window sizes include 0, 5, 15, 25, 35, and 45, where 0 stands for no MWA processing. After applying MWA on the experimental RSSI sequences, we calculated the new intact key information ratio using (12). Table 5 and Table 6 show the results for indoor and outdoor experiments, respectively.

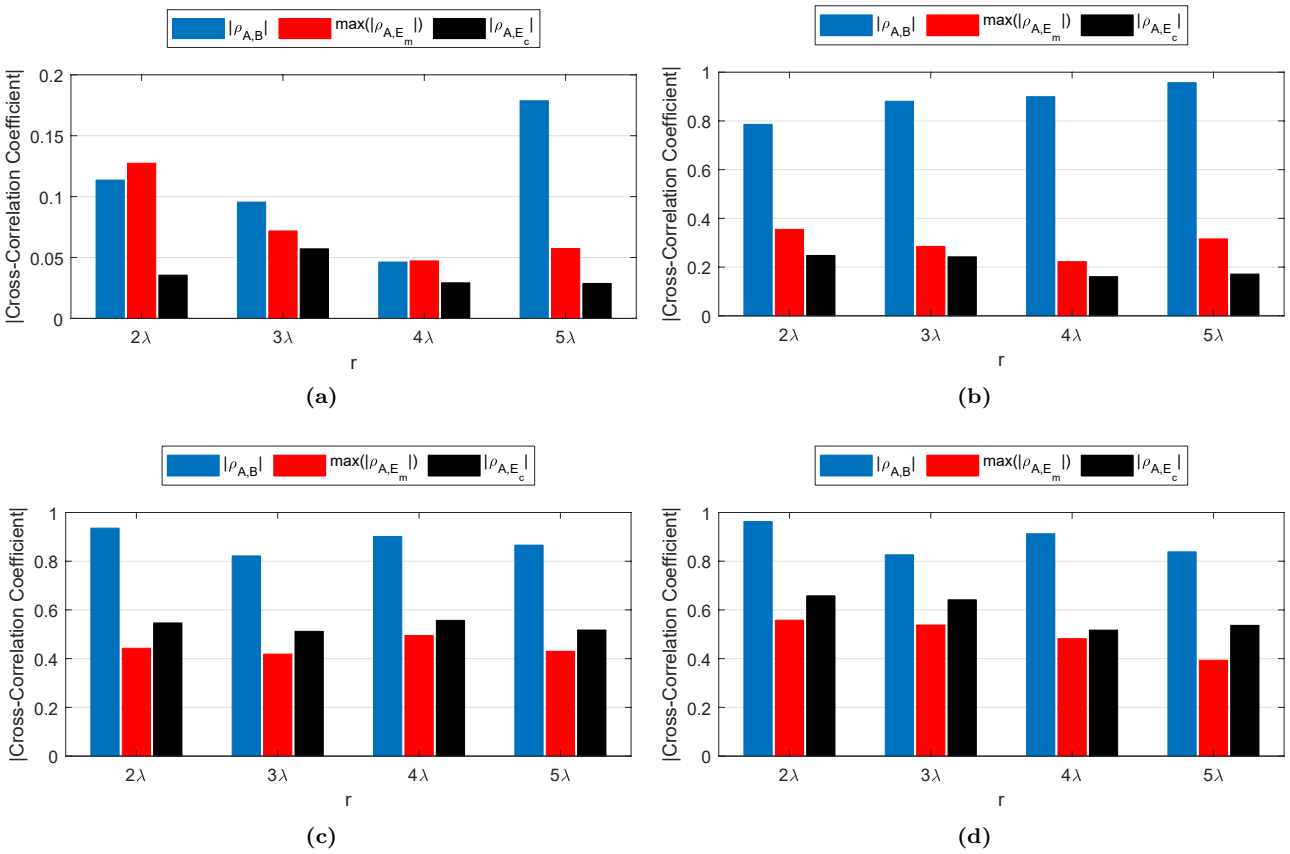

Fig. 4. Cross-correlation results in indoor experiments. $|\rho_{A,B}|$ denotes the absolute Pearson correlation coefficient between Alice and Bob. $\max(|\rho_{A,E_m}|)$ denotes the maximum coefficient between Alice and eavesdroppers. $|\rho_{A,E_c}|$ denotes the coefficient between Alice and the colluding-eavesdropping attack. (a) Static scenario (Ia). (b) Channel with moving scatterers (Ib). (c) Channel with moving Bob (Ic). (d) Channel with moving Bob and moving scatterers (Id).

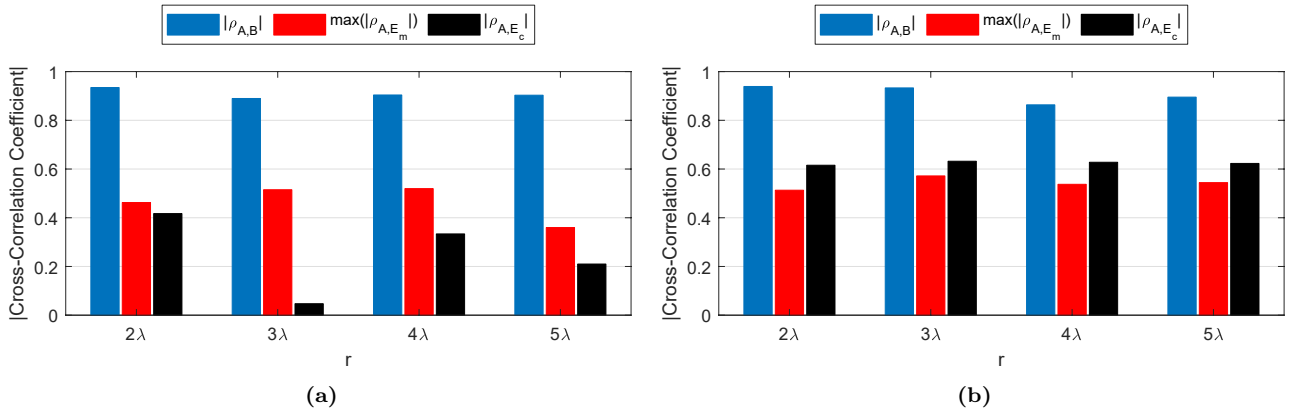

Fig. 5. Cross-correlation results in outdoor experiments. (a) Channel with moving scatterers (Ob). (b) Channel with moving Bob and moving scatterers (Od).

As can be observed from Table 5, in the scenarios (Ib), (Ic), and (Id), the intact key information ratio reduces as the MWA window size increases. The reduction is significant in the large-scale fading varying scenarios, e.g., (Ic) and (Id). The average reduction is 2.32% without large-scale fading variation and 9.77% with large-scale fading variation. From Table 6, the average reduction is 2.86% for large-scale fading invariant scenarios and 11.52% for varying large-scale fading scenarios in the outdoor experiments.

We deduce that the reason for the more significant reduction is that the MWA reduces noise and small-scale fad-

Table 3. Secret Key Capacity in Indoor Experiments

Scenario	r	$I(X_A;X_B)$	$I(X_A;X_B\|X_{E_1})$	$I(X_A;X_B\|X_{E_2})$	$I(X_A;X_B\|X_{E_3})$	$I(X_A;X_B\|X_{E_4})$	$I(X_A;X_B\|X_{E_c})$
(Ia)	5λ	0.0293	0.0297	0.0237	0.0289	0.0282	0.0273
	4λ	0.0225	0.0081	0.0187	0.0223	0.0126	0.0233
	3λ	0.0110	0.0084	0.0089	0.0064	0.0092	0.0095
	2λ	0.0160	0.0129	0.0151	0.0143	0.0111	0.0127
(Ib)	5λ	1.2830	1.2024	1.2310	1.2706	1.2634	1.2543
	4λ	1.0166	0.9954	0.9647	0.9967	0.9596	0.9624
	3λ	0.9167	0.9046	0.9019	0.8439	0.8437	0.8487
	2λ	0.5888	0.5475	0.4988	0.5233	0.5873	0.5241
(Ic)	5λ	0.8479	0.7487	0.7396	0.7474	0.7446	0.6714
	4λ	1.0165	0.8802	0.8988	0.8573	0.9376	0.8028
	3λ	0.7744	0.6776	0.7080	0.6731	0.6685	0.6014
	2λ	1.1411	1.0241	1.0024	1.0216	1.0246	0.9156
(Id)	5λ	0.7600	0.6784	0.6860	0.6777	0.6638	0.5723
	4λ	1.0533	0.9055	0.9239	0.9512	0.9850	0.8601
	3λ	0.7013	0.5619	0.5256	0.5542	0.5695	0.4366
	2λ	1.3026	1.0578	1.0565	1.1360	1.0934	0.9293

Table 4. Secret Key Capacity in Outdoor Experiments

Scenario	r	$I(X_A;X_B)$	$I(X_A;X_B\|X_{E_1})$	$I(X_A;X_B\|X_{E_2})$	$I(X_A;X_B\|X_{E_3})$	$I(X_A;X_B\|X_{E_4})$	$I(X_A;X_B\|X_{E_c})$
(Ob)	5λ	0.7933	0.7657	0.6987	0.7684	0.7506	0.7665
	4λ	0.7864	0.5621	0.6858	0.7509	0.7566	0.6711
	3λ	1.0384	1.0133	0.8552	1.0295	0.9181	1.0284
	2λ	0.9759	0.9315	0.8663	0.7616	0.9324	0.8034
(Od)	5λ	0.9215	0.8117	0.7628	0.7474	0.7302	0.6365
	4λ	0.8361	0.7123	0.6647	0.6741	0.7556	0.5786
	3λ	1.0646	0.9414	0.9027	0.8428	0.9591	0.7822
	2λ	1.1463	0.9958	0.9758	0.9736	1.0191	0.8612

Table 5. Intact Key Information Ratio Analysis Results of an MWA Application in Indoor Experiments

Scenario	r	$W.Size(0)$	$W.Size(5)$	$W.Size(15)$	$W.Size(25)$	$W.Size(35)$	$W.Size(45)$	$\Delta[W.Size(45),(0)]$
(Ia)	5λ	80.88%	76.89%	77.21%	75.35%	72.39%	71.97%	−8.91%
	4λ	36.17%	61.09%	55.47%	49.35%	40.72%	47.21%	+11.04%
	3λ	58.75%	77.94%	91.07%	51.98%	74.93%	80.76%	+22.01%
	2λ	69.36%	76.78%	84.35%	83.91%	83.85%	82.91%	+13.55%
(Ib)	5λ	93.72%	93.85%	93.62%	92.21%	91.13%	90.64%	−3.08%
	4λ	94.39%	94.61%	94.12%	93.10%	92.45%	92.13%	−2.26%
	3λ	92.04%	91.65%	91.36%	89.88%	89.49%	88.60%	−3.44%
	2λ	85.95%	85.74%	85.05%	85.21%	85.60%	85.46%	−0.49%
(Ic)	5λ	79.18%	79.15%	77.69%	74.60%	71.27%	68.75%	−10.43%
	4λ	78.98%	78.37%	75.91%	74.21%	71.58%	69.34%	−9.64%
	3λ	77.66%	77.68%	76.80%	74.10%	71.99%	70.49%	−7.17%
	2λ	80.24%	79.46%	76.62%	73.15%	71.10%	69.76%	−10.48%
(Id)	5λ	75.30%	74.97%	72.76%	69.86%	66.34%	64.67%	−10.63%
	4λ	81.66%	80.69%	79.69%	77.21%	75.02%	74.42%	−7.24%
	3λ	62.25%	61.52%	62.07%	58.43%	53.72%	50.05%	−12.20%
	2λ	71.34%	71.09%	67.87%	65.20%	63.39%	61.00%	−10.34%

Table 6. Intact Key Information Ratio Analysis Results of an MWA Application in Outdoor Experiments

Scenario	r	$W.Size(0)$	$W.Size(5)$	$W.Size(15)$	$W.Size(25)$	$W.Size(35)$	$W.Size(45)$	$\Delta[W.Size(45),(0)]$
(Ob)	5λ	88.08%	88.01%	86.20%	86.34%	85.57%	86.15%	−1.93%
	4λ	71.47%	74.60%	74.79%	72.06%	70.13%	70.06%	−1.41%
	3λ	80.43%	81.21%	80.79%	80.16%	78.66%	77.09%	−3.34%
	2λ	78.04%	78.43%	76.99%	76.06%	73.61%	73.30%	−4.74%
(Od)	5λ	69.07%	68.80%	67.34%	63.89%	62.01%	62.10%	−6.97%
	4λ	69.20%	68.56%	65.47%	62.60%	59.29%	57.47%	−11.73%
	3λ	73.47%	73.15%	69.04%	65.37%	62.97%	60.73%	−12.74%
	2λ	75.12%	74.05%	70.41%	65.73%	62.87%	60.48%	−14.64%

ing at the same time. In the scenarios (Ic), (Id), and (Od), the small-scale fading reduction makes large-scale fading variation contribute to a higher portion of the channel information shared between key generation users. Hence, the colluding-eavesdropping attack can take advantage of the large-scale fading estimation to obtain more users' mutual information. Therefore, we argue that noise canceling-based signal pre-processing helps reduce the channel prob-

ing cost may not be optimal for the key generation channels with varying large-scale fading and small-scale fading effects.

6. A Conditional Entropy and High-Pass Filtering Countermeasure

Small-scale fading is more random than large-scale fading because it can be affected by slight movements. Hence, the key generation security can be improved against the colluding-eavesdropping attack if we can mitigate the large-scale fading and mainly leverage small-scale fading.

6.1. Countermeasure

Large-scale fading varies in a much slower manner compared to small-scale fading variation. This inspires us to devise a high-pass filtering approach to minimize the impact of large-scale fading variation. Discrete cosine transform (DCT) is commonly used in signal processing nowadays, and DCT-II is regarded as the most common DCT variant [50], which is adopted in this paper. To the best knowledge of the authors, this is *the first key generation study regarding filtering low-frequency components*, while the other research focuses on filtering high-frequency components [45, 49, 51, 52].

Identifying large-scale fading associated low-frequency components is of importance as excessive filtering leads to a significant secret key capacity drop. Therefore, we designed an algorithm exploiting conditional entropy to estimate the optimal filter size, as shown in Algorithm 1. Without loss of generality, we assume Bob will be responsible for the estimation and will send the estimated filter size to Alice. Both users will then carry out the DCT-based filtering.

Specifically, Bob will first transform his RSSI sequence to a sum of cosine components at different frequencies using DCT-II expression (line 1), given as

$$Y_u(z) = \sum_{n=1}^{N} X_u(n) \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)z\right], z = 0, ..., N-1 \tag{13}$$

Bob then sets $Y_B(z)$, $z = 1, 2, ..., Z$, as zero to cumulatively remove the low-frequency components (line 3). Subsequently, an inverse discrete cosine transform (IDCT) is used to transform the new Y_B back to a filtered RSSI sequence, $X^f_{B,z}$ (line 4). After that, Bob will calculate the conditional entropy $\mathbb{H}(X_B|X^f_{B,z})$ (line 5), which increases with filtered components. The increasing rate, denoted by $\nabla\mathbb{H}(X_B|X^f_{B,z})$, is not constant because large-scale fading changes more significantly than small-scale fading in magnitude. Bob will find the position of the largest increasing rate. The determined optimal filter size denoted by z_0, is the largest rate position added by one (line 6), as the increasing rate is calculated on a midpoint. Bob will send z_0 to Alice (line 7). Finally, Alice and Bob can obtain the filtered sequences, X^f_{A,z_0}, X^f_{B,z_0}, respectively (line 8).

Algorithm 1: Large-Scale Fading Filtering Algorithm.

Input: X_A,X_B %RSSI sequences of Alice and Bob
Input: Z % Maximum filter size
Output: X^f_{A,z_0},X^f_{B,z_0} %Filtered RSSI sequences
1 $Y_B = DCT(X_B)$
2 **for** $z \leftarrow 1$ ***to*** Z **do**
3 $\quad Y_B(z) = 0$
4 $\quad X^f_{B,z} = IDCT(Y_B)$
5 $\quad$ Bob calculates $\mathbb{H}(X_B|X^f_{B,z})$
6 $z_0 = \underset{z}{\operatorname{argmax}} \nabla\mathbb{H}(X_B|X^f_{B,z}) + 1$
7 Bob sends z_0 to Alice
8 Alice and Bob calculate large-scale fading filtered sequences, X^f_{A,z_0} and X^f_{B,z_0}, respectively.

6.2. Filtering Effect

We use (9) and (12) to analyze secret key capacity and intact key information ratio for filtered RSSI sequences, which are denoted by C^f_K and $R^f_{C_K}$, respectively. We considered two cases.

1. A worst-case scenario assumes that eavesdroppers know all the filtered components and develop the same filtering process as Alice and Bob.
2. A general case assumes that eavesdroppers have no knowledge about the filtered components.

Fig. 6 shows the high-pass filtering result for an outdoor large-scale fading varying channel. The resulted secret key capacities in both general and worst cases are significantly improved, with the maximum improvement occurs after filtering the first nine components. When more components are filtered, the secret key capacities start to drop. The secret key capacity improvement is contributed by the elimination of large-scale fading variation, which reduces the channel correlation between the colluding-eavesdropping attack and legitimate users. After filtering the first seventy components, the secret key capacities go below the original value. This is because the high-pass filter starts to affect small-scale fading, and the entire entropy of the RSSI sequences is reduced. Fig. 7 shows the high-pass filtering result for outdoor channels without large-scale fading variation, i.e., scenario (Ob). As there was no large-scale fading, the resulted secret key capacity is almost always smaller than the original capacity. This is caused by entropy reduction as filtered components are associated with small-scale fading.

As can be observed in Fig. 6, an optimal secret key capacity can be achieved by filtering the first $z_0 = 9$ components. This is obtained by knowing all RSSI sequences of Alice, Bob, and eavesdroppers. However, this cannot be done in practice as Alice and Bob are not allowed to exchange their measured RSSI sequences. Furthermore, they do not have access to the RSSI sequences of eavesdroppers. Therefore, we carried out Algorithm 1 to let Bob develop large-scale fading filtering base on his RSSI observations. Figs. 8(a), (b), and (c) show the estimated z_0 in

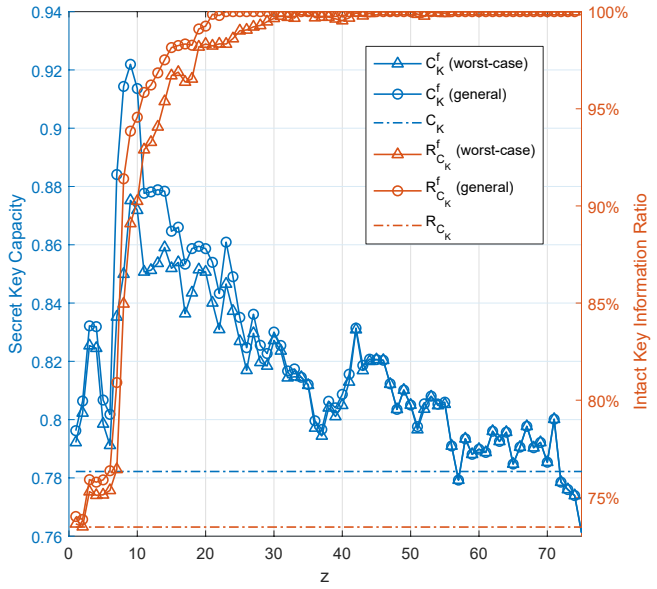

Fig. 6. Secret key capacity and intact key information ratio after filtering low-frequency components of the RSSI sequences measured in the scenario (Od) with $r = 3\lambda$.

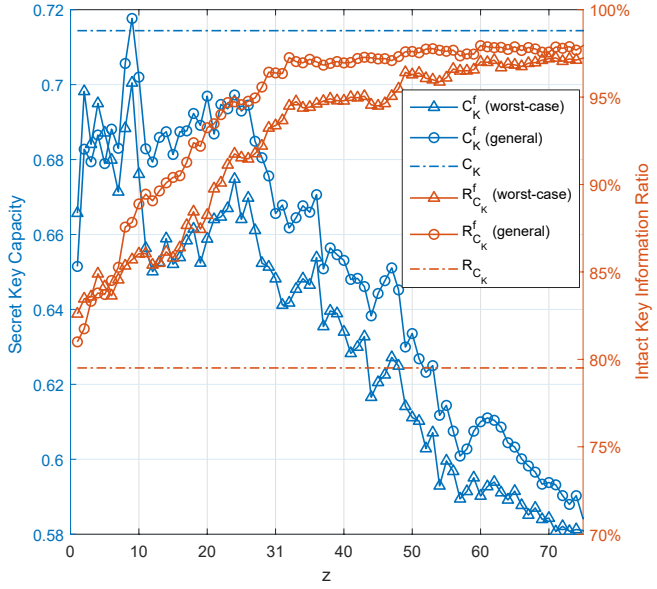

Fig. 7. Average secret key capacity and intact key information ratio after filtering low-frequency components of the RSSI sequences measured in the scenario (Ob).

the scenario (Od) when $r = 5\lambda$, $r = 4\lambda$, and $r = 2\lambda$. The estimated z_0 are 8, 7, and 7, respectively. All the resulted secret key capacities from the z_0 are higher than the original secret key capacities. Although Alice and Bob choose z_0 without knowing eavesdroppers' information, they can achieve a secret key capacity closing to the optimal value.

6.3. Key Disagreement Rate and Randomness

We implemented a mean-based quantizer to convert RSSI sequences into key bits. A mean value-based quantizer is mathematically given as follows

$$K_u(i) = \begin{cases} 1, & X_u(n) > \mu_u \\ 0, & X_u(n) \leq \mu_u \end{cases} \tag{14}$$

where $\mu_u = E\{X_u\}$ is the mean value. Before quantization, we downsampled experimental RSSI sequences to generate key bits with length, l_k. The RSSI measurements were dropped probabilistically to maintain a high bit entropy under the mean value-based quantizer. A multi-region quantizer can be deployed without downsampling the RSSI sequences while maintaining a high bit entropy [53, 54].

Key disagreement rate (KDR) and randomness are common evaluation metrics in the key generation area [8]. KDR is defined as the ratio between the numbers of different key bits and total key bits, expressed as

$$KDR_{u,v} = \frac{\sum_{n=1}^{l_k} |K_u(n) - K_v(n)|}{l_k} \tag{15}$$

The values of KDR should close to 0 when keys are associated with legitimate users and close to 0.5 when associated with eavesdroppers. The tolerable KDR is determined by the following information reconciliation stage, which will correct key bit mismatches using error-correcting codes. The correcting capacity of information reconciliation depends on the adopted error correction code. A correction capacity of 0.2 is used in this paper [39].

Table 7. KDR Before and After Large-Scale Fading Filtering

Scenario	r	$KDR_{A,B}$		KDR_{A,E_c}	
		Before	After	Before	After
(Od)	5λ	0.1026	0.1359	0.2456	0.4798
	4λ	0.1055	0.1424	0.2581	0.4870
	3λ	0.0798	0.1078	0.2563	0.4891
	2λ	0.0708	0.1056	0.2524	0.4943

Table 7 shows the KDR results, where eavesdroppers developed the same large-scale fading filtering process as Alice and Bob. All KDR increased as large-scale fading was filtered. However, the KDR associated with the colluding-eavesdropping attack increased more significantly than those of legitimate users. The KDR between legitimate users is all within 0.2, hence they can correct the mismatches. On the other hand, the KDR associated with eavesdroppers is close to 0.5, hence comparable to a random guess.

We used the National Institute of Standard and Technology (NIST) randomness test suite to evaluate the randomness of key bits generated from filtered RSSI sequences. Each test returns a p-value, and the test passes if the p-value is larger than 0.01. We run eight widely used NIST tests in physical layer key generation systems [18, 20, 32, 39, 53, 55]. The randomness test results of the key bits generated by Bob after large-scale fading filtering is shown in Table 8, and all eight tests passed.

Overall, as a security recommendation and an effective countermeasure against our revealed new attack, a

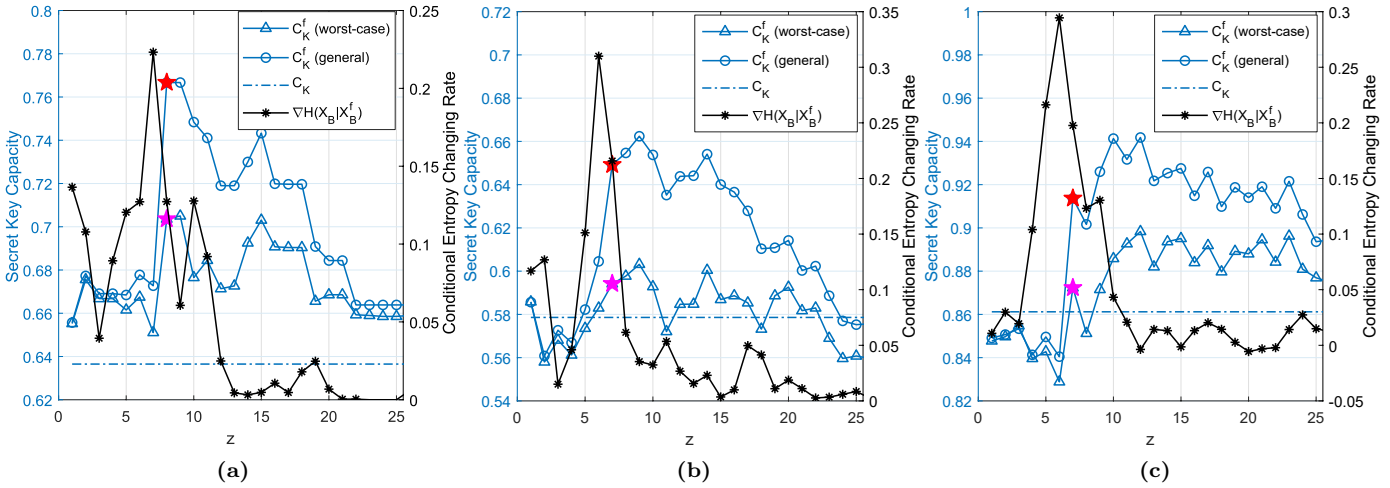

Fig. 8. The optimal filter size, z_0, estimated with Bob's RSSI measurements. The star denotes the secret key capacity after implementing the corresponding optimal filter in the scenario (Od), where the red star denotes the general case, and the pink star denotes the worst case. (a) $r = 5\lambda$. (b) $r = 4\lambda$. (c) $r = 2\lambda$.

Table 8. Randomness Test Results of Large-Scale Fading Filtered Key Bits Generated by Bob

Scenario	(Od)			
r	5λ	4λ	3λ	2λ
Sequence Length	413	431	441	396
Frequency	0.146	0.104	0.134	0.204
Block Frequency	0.219	0.265	0.245	0.362
Runs	0.057	0.105	0.054	0.547
Longest Run of 1s	0.035	0.138	0.107	0.461
FFT	0.359	0.819	0.731	0.791
Serial	0.499 0.079	0.499 0.499	0.841 0.922	0.499 0.499
Appro. Entropy	0.076	0.170	0.390	0.386
Cum. Sums (rev)	0.157	0.122	0.122	0.408
Cum. Sums (fwd)	0.149	0.140	0.160	0.167

high-pass filter can be implemented with Algorithm 1 to effectively minimize the secret key information leak caused by large-scale fading variation in practice.

7. Conclusion

This paper investigated physical layer key generation security when both large-scale and small-scale fading are presented. In particular, we constructed a long-range communications key generation testbed and carried out extensive experiments in indoor and outdoor environments. A new attack that perceives large-scale fading effects was revealed and formalized, using only four eavesdroppers circularly around a legitimate user. We demonstrated that the RSSI sequences generated in a large-scale fading varying channel are more predictable than no large-scale fading variation through the cross-correlation and secret key capacity analysis. Therefore, a higher portion of secret keys can be compromised under the revealed attack. Furthermore, through the intact key information ratio analysis, we found that the revealed attack's capability can be boosted by signal pre-processing techniques designed initially to improve channel probing reciprocity for generating highly agreed key bits. Finally, we proposed a conditional entropy and high-pass filtering countermeasure for the revealed attack as the impact of large-scale fading variation persists for a long duration. In this context, we designed an algorithm to allow key generation users to adaptively estimate the large-scale fading associated low-frequency components based on their channel observations. The results demonstrated that the countermeasure can significantly improve the users' secret key capacity and increase eavesdroppers' KDR almost twice under the large-scale fading resulted key generation attack. The NIST randomness test suite confirmed that the randomness of the filtered key sequences is suitable for cryptographic applications.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surveys Tuts. 17 (4) (2015) 2347–2376. doi:10.1109/COMST.2015.2444095.

[2] J. Granjal, E. Monteiro, J. S. Silva, Security for the Internet of things: A survey of existing protocols and open research issues, IEEE Commun. Surveys Tuts. 17 (3) (2015) 1294–1312. doi:10.1109/COMST.2015.2388550.

[3] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, A. S. M. Nainar, N. M. Akim, M. Imran, Deep learning and big data technologies for IoT security, Comput. Commun. 151 (2020) 495–517. doi:10.1016/j.comcom.2020.01.016.

[4] K. Zeng, Physical layer key generation in wireless networks: Challenges and opportunities, IEEE Commun. Mag. 53 (6) (2015) 33–39. doi:10.1109/MCOM.2015.7120014.

[5] J. Buchmann, A. May, U. Vollmer, Perspectives for cryptographic long-term security, Commun. ACM 49 (9) (2006) 50–55. doi:10.1145/1151030.1151055.

[6] Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: Technical challenges, recent advances, and future trends, Proc. IEEE 104 (9) (2016) 1727–1765. doi:10.1109/JPROC.2016.2558521.

[7] C. Cheng, R. Lu, A. Petzoldt, T. Takagi, Securing the Internet of things in a quantum world, IEEE Commun. Mag. 55 (2) (2017) 116–120. doi:10.1109/MCOM.2017.1600522CM.

[8] J. Zhang, T. Q. Duong, A. Marshall, R. Woods, Key generation from wireless channels: A review, IEEE Access 4 (2016) 614–626. doi:10.1109/ACCESS.2016.2521718.

[9] M. Bottarelli, G. Epiphaniou, D. K. B. Ismail, P. Karadimas, H. Al-Khateeb, Physical characteristics of wireless communication channels for secret key establishment: A survey of the research, Comput. Secur. 78 (2018) 454–476. doi:10.1016/J.COSE.2018.08.001.

[10] Q. Hu, J. Zhang, A. Mitrokotsa, G. Hancke, Tangible security: Survey of methods supporting secure ad-hoc connects of edge devices with physical context, Comput. Secur. 78 (2018) 281–300. doi:10.1016/J.COSE.2018.06.009.

[11] J. Zhang, S. Rajendran, Z. Sun, R. Woods, L. Hanzo, Physical layer security for the Internet of things: Authentication and key generation, IEEE Wireless Commun. 26 (5) (2019) 92–98. doi:10.1109/MWC.2019.1800455.

[12] R. Ahlswede, I. Csiszár, Common randomness in information theory and cryptography-Part I: Secret sharing, IEEE Trans. Inf. Theory 39 (4) (1993) 1121–1132. doi:10.1109/18.243431.

[13] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, N. B. Mandayam, Information-theoretically secret key generation for fading wireless channels, IEEE Trans. Inf. Forensics Security 5 (2) (2010) 240–254. doi:10.1109/TIFS.2010.2043187.

[14] C. T. Zenger, M. Pietersz, J. Zimmer, J.-F. Posielek, T. Lenze, C. Paar, Authenticated key establishment for low-resource devices exploiting correlated random channels, Comput. Netw. 109 (2016) 105–123. doi:10.1016/J.COMNET.2016.06.013.

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

[16] Y. Wei, K. Zeng, P. Mohapatra, Adaptive wireless channel probing for shared key generation based on PID controller, IEEE Trans. Mobile Comput. 12 (9) (2013) 1842–1852. doi:10.1109/TMC.2012.144.

[17] G. Epiphaniou, P. Karadimas, D. K. B. Ismail, H. Al-Khateeb, A. Dehghantanha, K.-K. R. Choo, Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social IoT networks, IEEE Internet Things J. 5 (4) (2017) 2496–2505. doi:10.1109/JIOT.2017.2764384.

[18] J. Zhang, A. Marshall, R. Woods, T. Q. Duong, Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers, IEEE Trans. Commun. 64 (6) (2016) 2578–2588. doi:10.1109/TCOMM.2016.2552165.

[19] J. Zhang, M. Ding, D. López-Pérez, A. Marshall, L. Hanzo, Design of an efficient OFDMA-based multi-user key generation protocol, IEEE Trans. Veh. Technol. 68 (9) (2019) 8842–8852. doi:10.1109/TVT.2019.2929362.

[20] H. Liu, Y. Wang, J. Yang, Y. Chen, Fast and practical secret key extraction by exploiting channel response, in: Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM), Turin, Italy, 2013, pp. 3048–3056. doi:10.1109/INFCOM.2013.6567117.

[21] J. W. Wallace, R. K. Sharma, Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis, IEEE Trans. Inf. Forensics Security 5 (3) (2010) 381–392. doi:10.1109/TIFS.2010.2052253.

[22] Z. Li, H. Wang, H. Fang, Group-based cooperation on symmetric key generation for wireless body area networks, IEEE Internet Things J. 4 (6) (2017) 1955–1963. doi:10.1109/JIOT.2017.2761700.

[23] N. Aldaghri, H. Mahdavifar, Physical layer secret key generation in static environments, IEEE Trans. Inf. Forensics Security 15 (2020) 2692–2705. doi:10.1109/TIFS.2020.2974621.

[24] M. F. Haroun, T. A. Gulliver, Secret key generation using chaotic signals over frequency selective fading channels, IEEE Trans. Inf. Forensics Security 10 (8) (2015) 1764–1775. doi:10.1109/TIFS.2015.2428211.

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

[26] M. Edman, A. Kiayias, Q. Tang, B. Yener, On the security of key extraction from measuring physical quantities, IEEE Trans. Inf. Forensics Security 11 (8) (2016) 1796–1806. doi:10.1109/TIFS.2016.2543687.

[27] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, Q. Xu, Experimental study on key generation for physical layer security in wireless communications, IEEE Access 4 (2016) 4464–4477. doi:10.1109/ACCESS.2016.2604618.

[28] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, C. Paar, The passive eavesdropper affects my channel: Secret-key rates under real-world conditions, in: Proc. IEEE Globecom TCPLS Workshops, Washington DC, USA, 2016, pp. 1–6. doi:10.1109/GLOCOMW.2016.7849064.

[29] C. D. T. Thai, J. Lee, T. Q. Quek, Physical-layer secret key generation with colluding untrusted relays, IEEE Trans. Wireless Commun. 15 (2) (2016) 1517–1530. doi:10.1109/TWC.2015.2491935.

[30] M. Waqas, M. Ahmed, Y. Li, D. Jin, S. Chen, Social-aware secret key generation for secure device-to-device communication via trusted and non-trusted relays, IEEE Trans. Wireless Commun. 17 (6) (2018) 3918–3930. doi:10.1109/TWC.2018.2817607.

[31] M. Waqas, M. Ahmed, J. Zhang, Y. Li, Confidential information ensurance through physical layer security in device-to-device communication, in: Proc. IEEE Global Commun. Conf. (GLOBECOM), Abu Dhabi, UAE, 2018, pp. 1–7. doi:10.1109/GLOCOM.2018.8647343.

[32] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel, in: Proc. 14th Annu. Int. Conf. Mobile Computing and Networking (MobiCom), San Francisco, California, USA, 2008, pp. 128–139. doi:10.1145/1409944.1409960.

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

[34] S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, R. Ricci, Secret key extraction using Bluetooth wireless signal strength measurements, in: Proc. 11th Annu. IEEE Int. Conf. Sensing, Commun., and Networking (SECON), Singapore, 2014, pp. 293–301. doi:10.1109/SAHCN.2014.6990365.

[35] K. Mekki, E. Bajic, F. Chaxel, F. Meyer, A comparative study of LPWAN technologies for large-scale IoT deployment, ICT Express 5 (1) (2019) 1–7. doi:10.1016/J.ICTE.2017.12.005.

[36] B. Miles, E.-B. Bourennane, S. Boucherkha, S. Chikhi, A study of LoRaWAN protocol performance for IoT applications in smart agriculture, Comput. Commun. 164 (2020) 148–157. doi:10.1016/j.comcom.2020.10.009.

[37] H. Ruotsalainen, S. Grebeniuk, Towards wireless secret key agreement with LoRa physical layer, in: Proc. ACM ARES, no. 23, Hamburg, Germany, 2018, pp. 1–6. doi:10.1145/3230833.3232803.

[38] W. Xu, S. Jha, W. Hu, Exploring the feasibility of physical layer key generation for LoRaWAN, in: Proc. IEEE Trustcom, New York, NY, USA, 2018, pp. 231–236. doi:10.1109/TRUSTCOM/BIGDATASE.2018.00044.

[39] J. Zhang, A. Marshall, L. Hanzo, Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks, IEEE Trans. Veh. Technol. 67 (12) (2018) 12462–12466. doi:10.1109/TVT.2018.2877201.

[40] W. Xu, S. Jha, W. Hu, LoRa-key: Secure key generation system for LoRa-based network, IEEE Internet Things J. 6 (4) (2019) 6404–6416. doi:10.1109/JIOT.2018.2888553.

[41] H. Ruotsalainen, J. Zhang, S. Grebeniuk, Experimental investigation on wireless key generation for low power wide area networks, IEEE Internet Things J. 7 (3) (2020) 1745–1755. doi:10.1109/JIOT.2019.2946919.

[42] J. Zhang, M. Ding, G. Li, A. Marshall, Key generation based on large scale fading, IEEE Trans. Veh. Technol. 68 (8) (2019) 8222–8226. doi:10.1109/TVT.2019.2922443.

[43] A. Khisti, S. N. Diggavi, G. W. Wornell, Secret-key agreement with channel state information at the transmitter, IEEE Trans. Inf. Forensics Security 6 (3) (2011) 672–681. doi:10.1109/TIFS.2011.2151188.

[44] F. Zhan, Z. Zhao, Y. Chen, N. Yao, On the using of Rényi's quadratic entropy for physical layer key generation, Comput. Commun. 137 (2019) 32–43. doi:10.1016/J.COMCOM.2019.02.001.

[45] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, D. Cao, High-agreement uncorrelated secret key generation based on principal component analysis preprocessing, IEEE Trans. Commun. 66 (7) (2018) 3022–3034. doi:10.1109/TCOMM.2018.2814607.

[46] S. Gopinath, R. Guillaume, P. Duplys, A. Czylwik, Reciprocity enhancement and decorrelation schemes for PHY-based key generation, in: Proc. IEEE Globecom TCPLS Workshops, Austin, TX, USA, 2014, pp. 1367–1372. doi:10.1109/GLOCOMW.2014.7063624.

[47] J. Zhang, R. Woods, A. Marshall, 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, 2015, pp. 1727–1731. doi:10.1109/ICASSP.2015.7178266.

[48] F. Zhan, N. Yao, Z. Gao, H. Yu, Efficient key generation leveraging wireless channel reciprocity for MANETs, J. Netw. Comput. Appl. 103 (2018) 18–28. doi:10.1016/j.jnca.2017.11.014.

[49] G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, P. Thomas, Efficient DCT-based secret key generation for the Internet of things, Ad Hoc Netw. 92. doi:10.1016/J.ADHOC.2018.08.014.

[50] N. Ahmed, T. Natarajan, K. R. Rao, Discrete cosine transform, IEEE Trans. Comput. 100 (1) (1974) 90–93. doi:10.1109/T-C.1974.223784.

[51] G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, P. Thomas, Physical layer secret-key generation with discreet cosine transform for the Internet of things, in: Proc. IEEE ICC, Paris, France, 2017, pp. 1–6. doi:10.1109/ICC.2017.7997419.

[52] F. Zhan, N. Yao, On the using of discrete wavelet transform for physical layer key generation, Ad Hoc Netw. 64 (2017) 22–31. doi:10.1016/j.adhoc.2017.06.003.

[53] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, S. V. Krishnamurthy, On the effectiveness of secret key extraction from wireless signal strength in real environments, in: Proc. 15th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom), Beijing, China, 2009, pp. 321–332. doi:10.1145/1614320.1614356.

[54] Q. Han, J. Liu, Z. Shen, J. Liu, F. Gong, Vector partitioning quantization utilizing K-means clustering for physical layer secret key generation, Inf. Sci. 512 (2020) 137–160. doi:10.1016/j.ins.2019.09.076.

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