On the Colluding Attack to Compromise Physical Layer Key Generation Through a Large-Scale Fading Estimation

Lu Yang\textsuperscript{1,*}, Yansong Gao\textsuperscript{2}, Seyit Camtepe\textsuperscript{2}, and Dhammika Jayalath\textsuperscript{1}

\textsuperscript{1}Queensland University of Technology, QLD 4000, Australia
\textsuperscript{2}CSIRO Data61, NSW 2122, Australia

Abstract

Wireless Sensor Network (WSN) is one of the major paradigms in the IoT world. Due to the hardware constraint, the Transport Layer Security (TLS) implementation on WSN is limited by the computational and key management overheads. While the arithmetic based algorithms are mathematically expensive, the wireless channel based Physical Layer Security (PLS) can provide lightweight solutions. Physical layer key generation is the lightweight key exchange attracting considerable researches in recent years. Most of the researches focus on the key agreement and the security to defend against active attacks. However, the passive attacks have not been widely investigated, as a spatial decorrelation assumption is commonly made to exclude the scenario that eavesdroppers can obtain correlated channel characteristics when they locate at more than a half carrier wavelength to legitimate users. We challenge the assumption by demonstrating that the changing large-scale fading in a mobile-to-fixed (M2F) channel leaks key information to the eavesdroppers. We propose the colluding-side-channel attack (colluding-SCA) to develop physical layer key inference experiments. We validate our claim by showing the theoretical analysis and experimental results. While the changing large-scale fading in a M2F channel leaks key information, a fixed-to-fixed (F2F) channel can defend against the colluding-SCA as large-scale fading does not change in such channel. We conclude that if a channel has large-scale fading variance that contributes to the physical layer key entropy, the eavesdroppers will have a higher key inference capacity. Signal pre-processing is widely investigated for its implementation on physical layer key generation to improve the key agreement. We extend our research to demonstrate that signal pre-processing can further increase the key inference capacity of eavesdroppers, with a moving window average (MWA) method as the research object to validate the claim.

Keywords—fixed-to-fixed channel, large-scale fading, mobile-to-fixed channel, physical layer key generation, small-scale fading, wireless sensor network

\textsuperscript{*}Corresponding author
Email address: L41.yang@hdr.qut.edu.au
1 Introduction

Applications of the Wireless Sensor Network (WSN) include health monitoring, environmental sensing, industrial control and military surveillance [1]. It is obvious there are demands to protect the WSN communications from eavesdropping. Encryption is one of the most important techniques to protect data transmissions. The regular update of cryptographic keys is essential to prevent a successful brute-force attack, and maintain forward secrecy [2]. Implementing Transport Layer Security (TLS) key exchange algorithms, like RSA (Rivest-Shamir-Adleman) and DH (Diffie-Hellman), on a WSN device is mathematically expensive, leading to a high power consumption problem [3]. These algorithms are computational security, which rely on complex arithmetic that brings significant overheads to the resource-constrained device. Although there are lightweight TLS algorithms, they do not provide information-theoretic security and they are vulnerable to the development of quantum computing [4–6]. Post-quantum key exchange is the viable solution to the threats in the presence of quantum computers. However, it does not alleviate the computational overheads, and it has efficiency and usability problems [7,8]. Further, the decentralized distribution of WSNs makes the key management using public key infrastructures (PKIs) not trivial in TLS. For example, both RSA and DH key change require new domain parameters after a given period to maintain secrecy.

In recent years, physical layer security (PLS) has attracted considerable research interests to provide lightweight security solutions [9–11]. Generating cryptographic keys at physical layer by exploiting the natural randomness of electromagnetic wave propagation can achieve information-theoretic security without a high computational capacity requirement. Among authenticated channels, physical layer key generation can generate cryptographic keys for single-hop and multi-hop WSNs without PKI aids [12,13].

Many PLS researches have been reported for improving the key agreement and generation rate at physical layer [14–22]. Some researches have been reported for the defending against active attacks [23,24]. However, the passive attack study and practical implementation are rather limited. In [25], an active channel attack in static environment key generation by introducing an intermediate object to repeatedly blocks and unblocks a line-of-sight path is proposed, but the security analysis is not shown. A study comprising mutual information and key generation rate metrics can be developed to build on the research. In [26], the theoretical secrecy outage probability (SOP) for $M$ colluding eavesdroppers is investigated for a multi-hop physical layer key generation scenario. In [27], a cooperative jamming technique is proposed to defend against eavesdroppers and enhance downlink transmissions. The SOP minimization is developed in theory. In [28], the first comparison of physical layer key generation implementations under explicit channel settings is developed. The implementations adopt LoRa devices, and the channel settings include static, low-speed dynamic, and high-speed dynamic scenarios.

In the physical layer key generation researches, a commonly made assumption is spatial decorrelation. Eavesdroppers locate more than a half carrier wave-
length to legitimate users experience different fading, resulting in uncorrelated channel characteristics. The eavesdroppers ability to infer the cryptographic keys is limited by the spatial discrepancy. However, we argue, the assumption is reliable if only small-scale fading contributes to key entropy. For a mobile-to-fixed (M2F) channel, large-scale fading also contributes to the entropy. Different from small-scale fading, large-scale fading is not random. Eavesdroppers can estimate the large-scale fading in order to infer the key information generated at physical layer. We demonstrate and validate the claim by proposing a colluding-side-channel attack (colluding-SCA) in theory and practice. While the key generation in a M2F channel is vulnerable to the colluding-SCA, a fixed-to-fixed (F2F) channel can defend against the attack, due to large-scale fading does not change and contribute to the key entropy in such channel.

A SCA is a type of non-invasive physical attack targeting network security. The attack exploits information leaked by hardware, rather than algorithm vulnerability. During a SCA, the hardware specifications of a device are not altered, so the attack is hard to detect without surveillance. For the WSN, the deployed devices are often huge in number, small in dimensions, and battery-powered. A SCA is threatening in this context, as adding surveillance modules on the devices significantly increases the network overheads [29]. There are considerable research efforts towards the TLS targeted SCA [30–33]. However, the PLS targeted SCA attracts little attentions.

To the best of our knowledge, there is no researches relate to the large-scale fading effect in physical layer key generation. The research of key generation in different channel settings analyzes the superposition of fading without controlling the fading types [28]. Our contributions include, firstly, we are the first group to investigate the impact of the large-scale fading information in physical layer key generation. We propose the colluding-SCA to develop significant experiments to evaluate the key capacity reduction. Secondly, we find a F2F channel yields similar key capacities as a M2F channel. However, physical layer key generation is more competent in a F2F channel, as the channel does not have large-scale fading variance to leak the key information. Thirdly, a moving window average (MWA) is a low complexity signal pre-processing method, which is investigated in physical layer key generation to improve the key agreement [34, 35]. We define a key capacity reduction ratio to evaluate the MWA implemented physical layer key generation performance. The result shows a positive correlation between the MWA window size and the proportion of leaked key information. For the same window size, the key capacity reduction is more significant in a M2F channel compared to a F2F channel.

The rest of the paper is organized as follows. Section 2 introduces the background of physical layer key generation. Section 3 introduces the signal and channel models we adopt in our theoretical analysis and experiments. We show the large-scale fading and small-scale fading simulations of the experimental environments. Section 4 introduces the proposed colluding-SCA, and the theoretical analysis for its ability to estimate the large-scale fading information at physical layer. Section 5 shows the experimental setup and metrics. Section 6 presents the experimental results and discussion. We use correlation and key
capacity analyses to show the colluding-SCA ability on key inference. We finally conclude our work in Section 7.

2 Physical Layer Key Generation

To perform key generation at physical layer, two legitimate users, say Alice and Bob, are required to alternatively send probing signals to the other. This step is called channel probing. Due to channel reciprocity, the exchanged signals experience the same fading, resulting in correlated received signal characteristics. According to the spatial decorrelation assumption, Alice and Bob can transmit probing signals in a public channel without the concern that an eavesdropper has the same characteristics, if the eavesdropper’s position is more than a half carrier wavelength to Alice and Bob. Received signal strength indicator (RSSI) is the most used received signal characteristic for key generation, as it is easy to measure.

In a quantization step, the measured RSSI samples can be converted to binary bits. A signal pre-processing method can be implemented to reduce bit disagreement prior to the quantization step. The most used methods include MWA, filtering [36], interpolation [37], and curve fitting [38]. A Gray coding implemented multilevel quantization scheme with error tolerances between the level thresholds can further reduce the bit disagreement [28].

An information reconciliation step is carried to detect and correct the bit mismatches after the quantization. It ensures two matched bit streams are generated on Alice and Bob’s sides. Error correcting codes like BCH code and low-density parity-check code are efficient to correct bit mismatches, but also leak some bit information.

A privacy amplification step is used to remove the leaked bits after the information reconciliation. In some cases, due to a high sampling rate, a bit stream may have clusters of ones or zeros. A hash function can be implemented to reduce the autocorrelation. At the end, the generated keys can be directly used in an AES encryption, or can be used as master keys to generate session

![Figure 1: Physical layer key generation implementing a SHA-256 in the privacy amplification.](image-url)
keys. A complete physical layer key generation exploiting RSSI is shown in FIGURE 1. An observation is the key information is exchanged in the channel probing and information reconciliation steps. They are the only steps which eavesdroppers can obtain key information by eavesdropping. However, a SCA can happen among all the steps.

3 Signal and Channel Models

FIGURE 2 demonstrates the signal transmission model in a fading channel. As \( u(t) \) is the baseband signal, the bandpass signal is \( s(t) = \text{Re}\{u(t)e^{j2\pi f_c t}\} \), where \( e^{j2\pi f_c t} \) is the carrier of frequency \( f_c \). The received signal is \( r(t) = \text{Re}\{v(t)e^{j2\pi f_c t}\} + z(t) \), where \( z(t) \) is the AWGN at the receiver, and \( v(t) \) is the baseband signal experienced the channel fading effect \( c(t) \). The expression is \( v(t) = u(t) * c(t) \), where \( * \) denotes convolution. \( c(t) \) is a superposition of large-scale fading and small-scale fading. For physical layer key generation, the channel reciprocity is reduced because of the discrepancy caused by \( z(t) \).

The expression of RSSI at the receiver is \( P_{\text{RSSI}}(t) = \frac{1}{\Delta T} \int_t^{t+\Delta T} |r'(t)|^2 \, dt \), where \( \Delta T \) is a RSSI sample duration. In our experiments, \( \Delta T \) is the duration of a LoRa physical layer message.

\[ P_r = P_t + K - 10\gamma \log_{10} \left( \frac{d}{d_0} \right) - \chi_{dB}, \tag{1} \]

where \( P_t \) is transmitter power, \( K \) is a value of combined system amplification parameters, such as antenna gains, \( \gamma \) is a path loss exponent, \( d_0 \) is a reference distance, \( d \) is the distance between a transmitter and a receiver, and \( \chi_{dB} \) is a log-normal distributed shadowing component with a zero mean \( (\mu_{\chi_{dB}} = 0) \). For a simple model, the shadowing variance, \( \sigma^2_{\chi_{dB}} \) is a constant over the distance \( d \). From the expression, large-scale fading is location-dependent and time-invariant. For a given location, large-scale fading is deterministic. FIGURE 3 shows a large-scale fading simulation. The transmitter power is 1 W. The carrier is 915 MHz. The signals travel 50 m with \( K = 0 \) dB, \( \gamma = 2 \), and \( \sigma^2_{\chi_{dB}} = 1 \).
Small-scale fading variance closely relates to subscriber and scatterer movements in a communication environment. The statistical model of the received signals experienced small-scale fading is

\[
    r(t) = \text{Re} \left\{ \sum_{n=0}^{N(t)} a_n(t) e^{-j\varphi_n(t)} u(t - \tau_n(t)) \right\} e^{j2\pi f_c t},
\]

where \( N \) is the total number of signal paths, \( n \) is a path index, \( a_n \) is amplitude attenuation, \( \varphi_n \) is a phase distortion, and \( \tau_n \) is a propagation delay. Small-scale fading is time-variant. The phase distortion expression is \( \varphi_n(t) = 2\pi f_c \tau_n(t) - \varphi_{D_n,0} \), where the first term is resulted from the propagation delay, and the second term is resulted from a Doppler frequency shift.

For a M2F channel, the Doppler frequency expression is \( f_D = \frac{v}{\lambda} \cos(\theta) \), where \( v_{si} \) is the speed of a moving subscriber, \( \theta \) is the angle of arrival, and \( \lambda \) is the carrier wavelength. For a F2F channel, the subscribers are stationary, the Doppler frequency is introduced by mobile scatterers. When transmitted signals approaching a scatterer, the scatterer acting as a moving receiver. After the signals engaging with the scatterer, the scatterer acting as a moving transmitter. As the result, a double Doppler frequency can be estimated by \( f_{\text{double}} = 2\frac{v_{sr}}{\lambda} \cos(\nu) \cos(\psi) \), where \( v_{sr} \) is the scatterer speed, \( \nu \) and \( \psi \) are the two arriving angles when signals approaching and leaving the scatterers surface. For a channel with a moving subscriber and moving scatterers, the total Doppler frequency can be estimated by \( f_{\text{total}} = f_D + f_{\text{double}} \).
FIGURE 4: Small-scale fading simulation. (a) Static channel. (b) Channel of moving scatterers. (c) Channel of a moving subscriber. (d) Channel of a moving subscriber and moving scatterers.

FIGURE 4 shows the small-scale fading simulation for a 915 MHz carrier. The maximum speed of moving scatterers is 1 m/s. The scatterers' speed follows the Weibull distribution with the definition of \( f(v_{sr}) = bv_{sr}^{a-1}e^{-\frac{bvsr}{a}} \), where \( a = 0.1 \) and \( b = 3.238 \). In FIGURE 4.(a), as no object is moving in the channel, the small-scale fading remains the same. The signals in FIGURE 4.(c) and FIGURE 4.(d) change more frequently than the signal in FIGURE 4.(b). It is because the channel without a moving subscriber has limited varying paths. This is also shown in our experimental results.

4 Colluding-Side-Channel Attack

We propose the colluding-SCA using a power averaging method to estimate large-scale fading information. Although there are other methods, the purpose of our research is to demonstrate the vulnerability of physical layer key generation when it involves with changing large-scale fading. We do not intend to find the most effective method to infer the key information.

As shown in FIGURE 5, Alice and Bob are the two legitimate subscribers in the physical layer key generation. They alternatively send probing signals and
measure the RSSI of received signals. There are four eavesdroppers uniformly locate at a distance $r$ to Alice. We assume that the distance ($d$) between Alice and Bob is much larger than the distance between Alice and the eavesdroppers ($d >> r$). WSN communication technologies like LoRa can reach a 10 km coverage, so it is feasible to assume far-field communications between Alice and Bob.

In a F2F channel, $d$ is a constant. Large-scale fading does not change in the channel, only small-scale fading contributes to the key entropy. In a M2F channel, $d$ changes as Bob moves. Both large-scale fading and small-scale fading contribute to the key entropy. The colluding-SCA can perform the large-scale fading estimation according to (1) in order to infer the key information. The proof is shown as follows.

The received signal strength at Alice resulted by the large-scale fading from Bob can be calculated by (1), where $P_t$ is the transmitting power of Bob.

$E$ eavesdroppers uniformly distribute around Alice with the distance $r$. The averaged received signal strength of the eavesdroppers by listening to Bob is

$$
Pr_E = \frac{1}{M} \sum_{m=1}^{M} \left\{ P_t B + K - 10\gamma \log_{10} \left( \frac{\sqrt{[d - r \cos (\alpha + \frac{2\pi m}{M})]^2 + [r \sin (\alpha + \frac{2\pi m}{M})]^2]}{d_0} - \chi dB \right) \right\},
$$

where $\alpha$ is the angle between the path of Alice and Bob and the path of Alice and an eavesdropper.

For log-normal shadowing,

$$
E(\chi dB) = 0,
$$
\[ P_{RE} = P_t B + K + \frac{1}{M} \sum_{m=1}^{M} \left\{ -10\gamma \log_{10} \left( \frac{\sqrt{d^2 + r^2 - 2dr \cos (\alpha + \frac{2\pi m}{M})}}{d_0} \right) \right\}. \]

Due to the uniform distribution,

\[ P_{RE} = P_t B + K - 10\gamma \log_{10} \left( \frac{\sqrt{d^2 + r^2}}{d_0} \right). \]

Due to \( d \gg r \),

\[ P_{RE} = P_t B + K - 10\gamma \log_{10} \left( \frac{d}{d_0} \right). \]

When \( \alpha = 0 \) and \( M \) is large, the error for the eavesdroppers to estimate the RSSI of Alice is upper bounded by \( |P_{RE} - P_{RA}| = |\chi_{dB}| \). The bounded error is resulted from the shadowing between Alice and Bob.

5 Experimental Setup and Metrics

We use practical implementations to validate the impact of the colluding-SCA. The hardware devices include six Arduino Nano controlled LoRa SX1276 chipsets. Each chipset connects to a laptop to record RSSI by using a serial port and a Python script. The recorded RSSI samples are then processed offline. Two of the devices acting as Alice and Bob, and the rest acting as the eavesdroppers. The chipsets operate on a 915 MHz band with a 500 kHz bandwidth. The LoRa chirp modulation spreading factor is 7. The code rate is 4/5. The resulted data rate is 21875 bps.

We consider four channel models, which include (a) a static channel, (b) a channel with moving scatterers, (c) a channel with a moving subscriber, and (d) a channel has both moving scatterers and a moving subscriber. For each of the channel model, we adjust the distance (\( r \)) between the eavesdroppers to Alice to develop four experiments. \( r \) includes 2\( \lambda \), 3\( \lambda \), 4\( \lambda \), and 5\( \lambda \), where \( \lambda \) is approximate 0.328 m. In each experiment, Alice and Bob alternatively sends probing signals to the other, meanwhile the four eavesdroppers passively receive the signals sent by Bob. We allow Alice and Bob to perform three-minute signal exchanges, resulting in at least 10000 RSSI samples in each experimental dataset.

Alice and the four eavesdroppers are in an indoor living environment, with a moderate number of scatterers and slow airflow. In the channel (a) experiments, we keep Bob and the objects in the environment stationary. In the channel (b) experiments, we create movements by allowing people to randomly walk and move large objects like chairs and desks in the environment. In the channel (c) experiments, we make Bob to walk while keep the other objects stationary. Bob randomly walks in an empty corridor with the distance (\( d \)) to Alice varying between 10 m to 40 m. Bob does not have line-of-sight paths with Alice and
the four eavesdroppers. In the channel (d) experiments, we make Bob to walk and create random movements at the same time.

We use correlation and mutual information (MI) to show physical layer key generation is vulnerable for the implementation in a M2F channel. The correlation expression is

\[ \rho_{X,Y} = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y}. \]  

(3)

The MI expression is

\[ I(X;Y) = H(X) - H(X|Y). \]  

(4)

A key capacity \((C_K)\) illustrates the largest achievable key generation rate. In theory, \(C_K\) is upper-bounded by the MI of legitimate subscribers and the conditional MI given by an eavesdropper.

\[ C_K = \min[I(X;Y), I(X;Y|Z)]. \]  

(5)

In our experiments, \(C_K\) can be expressed as

\[ C_K = \min[I(A;B), I(A;B|E_s), I(A;B|E_{SCA})]. \]  

(6)

where \(E_s\) with \(s = 1, 2, 3,\) or \(4\) represents the RSSI measured by a single eavesdropper, and \(E_{SCA}\) represents the RSSI measured by a group of four eavesdroppers performing the colluding-SCA.

For computing MI, we use the Pyitlib library with a maximum likelihood estimator. As Pyitlib takes discrete variables as inputs, we normalize the RSSI samples in all experimental dataset. Normalization is required by the quantization of a physical layer key generation implementation, as hardware gains can introduce undesired received signal strength thresholds that reduce the quantization efficiency.

6 Result and Discussion

In the following sections, we use the same channel model notations as shown in TABLE 1.

6.1 Correlation analysis

For brevity, as shown in FIGURE 6.(a), we extract 2000 normalized RSSI samples of Alice and Bob from a channel (a) experiment to show the practical RSSI pattern. Comparing to the simulation result in Section 3, the experimental RSSI has small variations caused by noise. The correlation of Alice and Bob is 0.046. The low correlation shows the RSSI at Alice is uncorrelated to the RSSI at Bob, and thus insufficient to generate matched keys. The low correlation is resulted by the limited temporal variation. FIGURE 6.(b) shows the example
| Notation | Channel Model                          | Entropy Source                      | Application |
|----------|----------------------------------------|-------------------------------------|-------------|
| (a)      | Static channel                         | Noise                               | -           |
| (b)      | Channel with moving scatterers         | Small-scale fading and noise        | F2F         |
| (c)      | Channel with moving Bob                | Large-scale fading, small-scale fading, and noise | M2F         |
| (d)      | Channel with moving Bob and moving scatterers | Large-scale fading, small-scale fading, and noise | M2F         |

FIGURE 6: Example RSSI samples measured in channels listed in TABLE 1.
FIGURE 7: Correlation analysis. i: $r = 5\lambda$. ii: $r = 4\lambda$. iii: $r = 3\lambda$. iv: $r = 2\lambda$.

of 2000 normalized RSSI samples from a channel (b) experiment. The correlation is 0.899, which is significantly improved by introducing small-scale fading variance. FIGURE 6.(c) shows the example of 2000 normalized RSSI samples from a channel (c) experiment. The correlation is 0.901. FIGURE 6. (d) shows
the example of 2000 normalized RSSI samples from a channel (d) experiment. The correlation is 0.913.

Comparing FIGURE 6.(b) and FIGURE 6.(d), it is obvious that the channel with a moving subscriber changes more frequently. As discussed in Section 3, this is due to Bob’s motion changes all channel paths, while the scatterers’ motion only changes partial paths. According to (2), small-scale fading is the summation of all channel paths, the less changed paths result in less variance.

FIGURE 7 shows the correlation analysis results of all experimental dataset. Each dataset contains at least 10000 RSSI samples. Correlations are calculated between Alice and Bob, Alice and each of the eavesdroppers, and Alice and the colluding-SCA. A correlation closes to one between Alice and Bob means highly matched keys can be generated at physical layer. A correlation closes to one associated with an eavesdropper means the eavesdropper can perform an accurate key inference.

From FIGURE 7, the low correlations are produced in the channel (a) experiments. The experiments with changing multipath produce the correlations close to 0.9. The eavesdroppers experience different fading, which results the lower correlations compared to Alice and Bob. The negative correlations in FIGURE 7.(a) are caused by noise. The negative correlations in FIGURE 7.(b) are caused by negatively related scatterer movements [42].

An observation is the colluding-SCA in channels (c) and (d) produces the higher correlations compared to each single eavesdroppers. In channels (a) and (b), the colluding-SCA does not provide benefits on the correlation improvement. In channels (c) and (d), the improved correlations are obtained by estimating the large-scale fading information. Comparing to the highest correlation provided by a signal eavesdropper, the colluding-SCA increases the correlation by around 25%. According to the theoretical analysis in Section 4, a larger number of colluding eavesdroppers can estimate large-scale fading more accurately. We expect the correlation improvement percentage increases if we add more eavesdroppers.

In channels (a) and (b), although the large-scale fading information is leaked to the colluding-SCA, it maintains the same value and does not contribute to key entropy all the time. Knowing the large-scale fading in channels (a) and (b) does not help the eavesdroppers to infer the keys.

6.2 Distance between Alice and the eavesdroppers

We use the R-squared ($R^2$) value to analyze the impact of the distances ($r$) between Alice and the eavesdroppers. $R^2 = 1$ represents a full key inference capacity by the eavesdroppers. We calculate $R^2$ by assuming the RSSI samples in each dataset received by Alice to be a time series, which can be modelled by a multiple linear regression equation comprising the four eavesdroppers as four explanatory variables. We use the Ordinary Least Square method to find the regression equation. We check the equation significance by using the F-test with a 0.95 significant level.
FIGURE 8: $R^2$ against the distance ($r$) between Alice and eavesdroppers.

The expression for calculating the R-squared values is

$$R^2 = 1 - \frac{\sum_{i=1}^{I}(\bar{RSSI}_i - RSSI_i)^2}{\sum_{i=1}^{I}(RSSI_i - \bar{RSSI}_i)^2},$$ \hspace{1cm} (7)

where $I$ is the number of RSSI samples in an experimental dataset, $i$ is a sample index, $RSSI_i$ is an experimental sample, $\bar{RSSI}_i$ is the average of all the samples in an experimental dataset, and $\bar{RSSI}_i$ is the predicted sample by a regression equation.

FIGURE 8 shows the $r$ and $R^2$ analysis result. The trends show $R^2$ decreases as $r$ increases. This is because small-scale fading decorrelation. The eavesdroppers locate farther to Alice obtain less correlated channel characteristics at physical layer. In channels (c) and (d), due to the large-scale fading variance, the eavesdroppers have higher key inference capacities, and thus do not need to approach Alice as closer to obtain highly correlated RSSI samples comparing to channels (a) and (b).

6.3 Key capacity analysis

We perform a key capacity ($C_K$) analysis to show large-scale fading variance does not improve the largest achievable rate for physical layer key generation. However, it makes the rate bounded by the colluding-SCA.

TABLE 2 shows the analysis result. The resulted $C_K$ with the unit of bits per sample for each experimental dataset is marked in red. The first observation
TABLE 2: Key capacity analysis result

| Channel Exp. No. | r   | $I(A;B)$ | $I(A;B|E_1)$ | $I(A;B|E_2)$ | $I(A;B|E_3)$ | $I(A;B|E_4)$ | $I(A;B|E_{SCA})$ |
|------------------|-----|----------|--------------|--------------|--------------|--------------|-----------------|
| (a)              | 1   | 5λ       | 0.0293       | 0.0297       | 0.0237       | 0.0289       | 0.0282          | 0.0273          |
|                  | 2   | 4λ       | 0.0225       | **0.0081**   | 0.0187       | 0.0223       | 0.0126          | 0.0233          |
|                  | 3   | 3λ       | 0.0110       | 0.0084       | 0.0089       | **0.0064**   | 0.0092          | 0.0095          |
|                  | 4   | 2λ       | 0.0160       | 0.0129       | 0.0151       | 0.0143       | **0.0111**      | 0.0127          |
| (b)              | 5   | 5λ       | 1.2830       | 1.2024       | 1.231        | 1.2706       | 1.2634          | 1.2543          |
|                  | 6   | 4λ       | 1.0166       | 0.9954       | 0.9647       | 0.9967       | **0.9596**      | 0.9624          |
|                  | 7   | 3λ       | 0.9167       | 0.9046       | 0.9019       | 0.8439       | 0.8437          | 0.8487          |
|                  | 8   | 2λ       | 0.5888       | 0.5475       | 0.4988       | 0.5233       | 0.5873          | 0.5241          |
| (c)              | 9   | 5λ       | 0.8479       | 0.7487       | 0.7396       | 0.7474       | 0.7446          | **0.6714**      |
|                  | 10  | 4λ       | 1.0165       | 0.8802       | 0.8988       | 0.8573       | 0.9376          | 0.8028          |
|                  | 11  | 3λ       | 0.7744       | 0.6776       | 0.7080       | 0.6731       | 0.6685          | 0.6014          |
|                  | 12  | 2λ       | 1.1411       | 1.0241       | 1.0024       | 1.0216       | 1.0246          | 0.9156          |
| (d)              | 13  | 5λ       | 0.7600       | 0.6784       | 0.6860       | 0.6777       | 0.6638          | 0.5723          |
|                  | 14  | 4λ       | 1.0533       | 0.9055       | 0.9239       | 0.9512       | 0.9850          | 0.8601          |
|                  | 15  | 3λ       | 0.7013       | 0.5619       | 0.5256       | 0.5542       | 0.5695          | 0.4366          |
|                  | 16  | 2λ       | 1.3026       | 1.0578       | 1.0565       | 1.1360       | 1.0934          | 0.9293          |

is the $C_K$ in channels (c) and (d) are all bounded by the colluding-SCA. While in channels (a) and (b), the colluding-SCA does not impact on the $C_K$. The smallest $C_K$ is in channel (a), which is 0.0064. This is because the noise source in (a) produces limited temporal variation. The largest $C_K$ is in channel (b), which is 1.2024, as (b) has the small-scale fading entropy source and can defend against the colluding-SCA.

The second observation is the channels with changing large-scale fading do not provide higher MI between Alice and Bob. In fact, $I(A;B)$ among all the channels have similar values except in channel (a). The observation suggests although a F2F channel is less variant than a M2F channel as shown in FIGURE 4 and FIGURE 6, the F2F channel can still provide a sufficient key generation rate at physical layer.

6.4 Signal pre-processing implemented physical layer key generation and colluding-SCA

We extend the colluding-SCA research by considering its effect on pre-processed RSSI samples. An MWA is effective to implement on physical layer key generation to improve the key agreement. It minimizes the need of information reconciliation. The expression for the MWA to find the means of previous $W$ RSSI samples is

$$MWA_i(RSSI) = \frac{1}{W} \sum_{q=0}^{W-1} RSSI_{i-q}.$$  (8)
We propose the key capacity reduction ratio \( R_K \) to illustrate the key capacity reduction caused by the colluding-SCA by using the following expression,

\[
R_K = \frac{I(A;B) - \min[I(A;B), I(A;B|E_s), I(A;B|E_{SCA})]}{I(A;B)}.
\]  

(9)

We use the common \( W \) values, including 5, 10, 15, 25, 35, and 45. \( W = 0 \) means no MWA implemented. FIGURE 9 shows the analysis result. For the experiments developed in channels (c) and (d), \( R_K \) significantly increases as \( W \) increases from 0 to 45. In (b), \( R_K \) increased by 0.0201 (22.3\%). In (c), \( R_K \) increased by 0.0941 (46.8\%). In (d), \( R_K \) increased by 0.1011 (36.8\%). The result for (a) is invalid to be shown as the aim of an MWA is signal denoising, and the signals in (a) are solely resulted by noise. From the analysis result, although a signal pre-processing can improve the key agreement at physical layer, it also reduces small-scale fading. For a M2F channel, the small-scale fading reduction makes the large-scale fading contributes to more key entropy. Therefore, the colluding-SCA can infer a higher proportion key information when it targets the signal pre-processing implemented physical layer key generation.

7 Conclusion

We propose the colluding-SCA to demonstrate and validate that large-scale fading variance in a M2F channel can be exploited by a group of eavesdroppers to infer the cryptographic keys generated at physical layer. The spatial decorrelation assumption in the physical layer key generation researches is unreliable
for the M2F channel implementation. We show that although a F2F channel has less varying channel paths for key generation compared to a M2F channel, it produces higher key capacities when the colluding-SCA presents in the channels. This is because the F2F channel has the sufficient entropy sources from small-scale fading, and it can defend against the colluding-SCA due to the absence of large-scale fading. We further demonstrate the key information leakage can be amplified in the signal pre-processing implemented physical layer key generation. While the signal pre-processing improves the key agreement, a higher proportion of the key capacity is lost due to large-scale fading contributes to more of the key entropy. The key capacity loss is more significant in a M2F channel compared to a F2F channel.

References

[1] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. Leung, “Recent advances in industrial wireless sensor networks toward efficient management in iot,” IEEE access, vol. 3, pp. 622–637, 2015.

[2] J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography. CRC press, 1996.

[3] K. Zeng, “Physical layer key generation in wireless networks: challenges and opportunities,” IEEE Communications Magazine, vol. 53, no. 6, pp. 33–39, 2015.

[4] J. Buchmann, A. May, and U. Vollmer, “Perspectives for cryptographic long-term security,” Communications of the ACM, vol. 49, no. 9, pp. 50–55, 2006.

[5] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, “Securing the internet of things in a quantum world,” IEEE Communications Magazine, vol. 55, no. 2, pp. 116–120, 2017.

[6] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” Proceedings of the IEEE, vol. 104, no. 9, pp. 1727–1765, 2016.

[7] D. J. Bernstein, “Introduction to post-quantum cryptography,” in Post-quantum cryptography, pp. 1–14, Springer, 2009.

[8] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, “Post-quantum key exchange: new hope,” in 25th {USENIX} Security Symposium ({USENIX} Security 16), pp. 327–343, 2016.

[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 Communications Magazine, vol. 53, no. 4, pp. 20–27, 2015.
[10] W. Trappe, “The challenges facing physical layer security,” *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[11] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, “Key generation from wireless channels: A review,” *IEEE Access*, vol. 4, pp. 614–626, 2016.

[12] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[13] L. J. Rodríguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, “Physical layer security in wireless cooperative relay networks: State of the art and beyond,” *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, 2015.

[14] 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 Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1278–1287, 2012.

[15] Q. Wang, K. Xu, and K. Ren, “Cooperative secret key generation from phase estimation in narrowband fading channels,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1666–1674, 2012.

[16] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, “Smokegrenade: An efficient key generation protocol with artificial interference,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1731–1745, 2013.

[17] P. Huang and X. Wang, “Fast secret key generation in static wireless networks: A virtual channel approach,” in *2013 Proceedings IEEE INFOCOM*, pp. 2292–2300, IEEE, 2013.

[18] M. Wilhelm, I. Martinovic, and J. B. Schmitt, “Secure key generation in sensor networks based on frequency-selective channels,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1779–1790, 2013.

[19] J. Zhang, A. Marshall, and L. Hanzo, “Channel-envelope differencing eliminates secret key correlation: Lora-based key generation in low power wide area networks,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12462–12466, 2018.

[20] G. Epiphanious, P. Karadimas, D. K. B. Ismail, H. Al-Khateeb, A. Delghantanaha, and K.-K. R. Choo, “Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social iot networks,” *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2496–2505, 2017.
[21] P. Linning, G. Li, J. Zhang, R. Woods, M. Liu, and A. Hu, “An investigation of using loop-back mechanism for channel reciprocity enhancement in secret key generation,” IEEE Transactions on Mobile Computing, vol. 18, no. 3, pp. 507–519, 2018.

[22] G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, and P. Thomas, “Efficient dct-based secret key generation for the internet of things,” Ad Hoc Networks, vol. 92, p. 101744, 2019.

[23] X. Zhou, B. Maham, and A. Hjorungnes, “Pilot contamination for active eavesdropping,” IEEE Transactions on Wireless Communications, vol. 11, no. 3, pp. 903–907, 2012.

[24] J. Xu, L. Duan, and R. Zhang, “Proactive eavesdropping via cognitive jamming in fading channels,” IEEE Transactions on Wireless Communications, vol. 16, no. 5, pp. 2790–2806, 2017.

[25] 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 Proceedings of the 15th annual international conference on Mobile computing and networking, pp. 321–332, ACM, 2009.

[26] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, “On secure wireless communications for iot under eavesdropper collusion,” IEEE Transactions on Automation Science and Engineering, vol. 13, no. 3, pp. 1281–1293, 2015.

[27] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, and X. Wang, “Cooperative jamming for physical layer security enhancement in internet of things,” IEEE Internet of Things Journal, vol. 5, no. 1, pp. 219–228, 2017.

[28] W. Xu, S. Jha, and W. Hu, “Lora-key: Secure key generation system for lora-based network,” IEEE Internet of Things Journal, 2018.

[29] I. Tudosa, F. Picariello, E. Balestrieri, L. De Vito, and F. Lamonaca, “Hardware security in iot era: the role of measurements and instrumentation,” in 2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4. 08/IoT), pp. 285–290, IEEE, 2019.

[30] P. C. Kocher, “Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems,” in Annual International Cryptology Conference, pp. 104–113, Springer, 1996.

[31] J. Bonneau and I. Mironov, “Cache-collision timing attacks against aes,” in International Workshop on Cryptographic Hardware and Embedded Systems, pp. 201–215, Springer, 2006.
[32] O. Acıı¸ cmez, Ç. K. Koç, and J.-P. Seifert, “Predicting secret keys via branch prediction,” in Cryptographers Track at the RSA Conference, pp. 225–242, Springer, 2007.

[33] J. Fan, X. Guo, E. De Mulder, P. Schaumont, B. Preneel, and I. Verbauwhede, “State-of-the-art of secure ecc implementations: a survey on known side-channel attacks and countermeasures,” in 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 76–87, IEEE, 2010.

[34] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio-telepathy: extracting a secret key from an unauthenticated wireless channel,” in Proceedings of the 14th ACM international conference on Mobile computing and networking, pp. 128–139, ACM, 2008.

[35] A. Soni, R. Upadhyay, and A. Kumar, “Wireless physical layer key generation with improved bit disagreement for the internet of things using moving window averaging,” Physical Communication, vol. 33, pp. 249–258, 2019.

[36] G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, and P. Thomas, “Physical layer secret-key generation with discrete cosine transform for the internet of things,” in 2017 IEEE International Conference on Communications (ICC), pp. 1–6, IEEE, 2017.

[37] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, “High-rate uncorrelated bit extraction for shared secret key generation from channel measurements,” IEEE Transactions on Mobile Computing, vol. 9, no. 1, pp. 17–30, 2009.

[38] A. Ambekar, M. Hassan, and H. D. Schotten, “Improving channel reciprocity for effective key management systems,” in 2012 International Symposium on Signals, Systems, and Electronics (ISSSE), pp. 1–4, IEEE, 2012.

[39] S. Thoen, L. Van der Perre, and M. Engels, “Modeling the channel time-variance for fixed wireless communications,” IEEE Communications letters, vol. 6, no. 8, pp. 331–333, 2002.

[40] A. Borhani and M. Pätzold, “Correlation and spectral properties of vehicle-to-vehicle channels in the presence of moving scatterers,” IEEE Transactions on Vehicular Technology, vol. 62, no. 9, pp. 4228–4239, 2013.

[41] P. Karadimas, E. D. Vagenas, and S. A. Kotsopoulos, “On the scatterers’ mobility and second order statistics of narrowband fixed outdoor wireless channels,” IEEE Transactions on Wireless Communications, vol. 9, no. 7, pp. 2119–2124, 2010.

[42] R. Dautov and G. R. Tsouri, “Effects of passive negative correlation attack on sensors utilizing physical key extraction in indoor wireless body area networks,” IEEE Sensors Letters, 2019.