Physical Layer-Based Secure Communications for Static and Low-Latency Industrial Internet of Things

Zijie Ji, Phee Lep Yeoh, *Member, IEEE,* Gaojie Chen, *Senior Member, IEEE,* Junqing Zhang, Yan Zhang, *Member, IEEE,* Zunwen He, *Member, IEEE,* Hao Yin, and Yonghui Li, *Fellow, IEEE*

***Abstract*—This paper proposes a wireless key generation solution for secure low-latency communications with active jamming attack prevention in wireless networked control systems (WNCS) of industrial Internet of Things (IIoT) applications. We first identify a new vulnerability in physical layer key generation schemes using wireless channel and random pilots (RP) in static environments. We derive a closed-form expression for the probability that the RP-based key is successfully attacked by a long-term eavesdropper at a fixed location. To prevent such attacks, we propose a one time pad (OTP) encrypted transmission solution assisted by one-way self-interference (SI), which has low-latency, high-security benefits, and active attack detection capability. The performance of the proposed scheme is analytically compared with two benchmark RP-based schemes, and its advantages are verified in a ray-tracing based simulation environment. We further investigate the impact of critical design parameters, which reveal fundamental insights for the deployment and implementation of our proposed secure communications scheme.**

***Index Terms*—Active attack detection, industrial Internet of Things, one time pad, physical layer key generation.**

I. Introduction

THANKS to the appealing features of low installation and maintenance costs for autonomous long-term operation, large numbers of sensors, actuators, controllers, and production equipment are being connected wirelessly to enable wireless networked control systems (WNCS) in industrial Internet of Things (IIoT) applications [1]. However, the broadcast nature of wireless communications poses challenging security threats to sensitive data transmissions. For example, eavesdropping, node tampering, and traffic analysis all compromise the confidentiality of the transmitted data [2], [3]. The protection of confidentiality in current IoT standards and protocols mainly uses public key cryptographic algorithms requiring high computation power and energy consumption, and thus is impractical for resource-constrained IoT devices in WNCS [4]. Furthermore, conventional public key solutions rely on solving challenging and time-consuming number-theoretic problems such as integer factorization, discrete logarithms, and elliptic curve cryptography, but they are vulnerable to eavesdroppers with quantum computers, which can quickly decode the key by using Shor's algorithm [5].

Physical layer wireless key generation has emerged as a promising technique to complement cryptography-based approaches [6], [7]. The main benefits of physical layer wireless key generation include its lightweight security implementation for resource-constrained IoT devices and its information-theoretically secure resistance to quantum attacks [8]. Specifically, through rapid pilot exchanges, the legitimate transceivers can extract the unpredictable randomness from their reciprocal wireless channels to generate shared keys. Meanwhile, the rapid spatial decorrelation process renders channel observations by any third party user to be uncorrelated with legitimate ones, thus protecting the generated keys from eavesdroppers. Given these advantages, extensive theoretical analysis [9]–[11] and experimental verification [12]–[14] have been dedicated to investigate the performance improvement and practical applicability of wireless key generation. In [9], subcarriers in orthogonal frequency-division multiplexing (OFDM) systems were employed to increase the key generation rate (KGR), and a novel amplitude and phase joint guard band scheme was proposed to minimize the key disagreement rate (KDR). In [10], the authors considered the use of multi-antenna spatial resources in the mesh topology to improve the group KGR. The authors in [11] proposed to enhance the KGR by optimizing the reflecting coefficients of an intelligent reflecting surface (IRS), where the correlation between legitimate channels was enhanced and their corresponding correlation with eavesdropping channels was weakened. In [12], a loop-back mechanism was designed to increase the channel reciprocity, and thus reduce the KDR. In [13], the correlation between channel samples was eliminated by using channel-envelope differencing, thereby maintaining the randomness of the generated keys. The authors in [14] investigated the impact of various protocol parameters on the security performance of generated keys in real environments. Although in-depth related researches have contributed to increasing KGR, reducing KDR, and ensuring randomness, three major problems still make it challenging to

This work was supported in part by the National Key R&D Program of China under Grant 2020YFB1804901; in part by the National Natural Science Foundation of China under Grant 61871035; in part by the ARC under Grant DP190101988 and DP210103410; and in part by the China Scholarship Council scholarship. *(Corresponding author: Yan Zhang.)*

Z. Ji, Y. Zhang, and Z. He are with the School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China (e-mail: {jizijie, zhangy, hezunwen}@bit.edu.cn).

P. L. Yeoh and Y. Li are with the School of Electrical and Information Engineering, University of Sydney, Sydney, NSW 2006, Australia (e-mail: {phee.yeoh, yonghui.li}@sydney.edu.au).

G. Chen is with the Institute for Communication Systems (ICS), 5GIC & 6GIC, University of Surrey, Guildford, Surrey GU2 7XH, U.K. (e-mail: gaojie.chen@surrey.ac.uk).

J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool L69 3GJ, U.K. (e-mail: junqing.zhang@liverpool.ac.uk).

H. Yin is with Institute of China Electronic System Engineering Corporation, Beijing 100141, China (e-mail: yinhao@cashq.ac.cn).

apply existing schemes to WNCS in IIoT.

First, applying wireless key generation in WNCS should consider the impact of static environments where the channel remains unchanged for a long time resulting in low KGR and security vulnerabilities. As the keys are obtained from channel characteristics, the update of keys relies on the movement of transceivers or fast changing wireless environments. Since most of the sensors and controllers in WNCS are fixed, the surrounding wireless environment will change very slowly, and thus the keys cannot be updated making them vulnerable to dictionary attacks [14]. To tackle this problem, artificial randomness can be introduced into the key generation process [15]–[20]. In [15], random beamforming was used to increase channel characteristic fluctuations by leveraging spatial diversity. However, the multi-antenna configuration at both the transmitter and receiver is not always feasible in resource-constrained IIoT networks, especially for low-cost sensors. Besides, auxiliary nodes, such as relays [16] or IRS [17], have also been considered to provide induced randomness, but additional deployment and coordination are required, and it is difficult to ensure the reliability of external devices. A promising solution to improve the KGR in static environments is the random pilot (RP) based approach, which operates without exploiting multiple antennas or extra helpers. It was first proposed in [18] and extended to broadband scenarios in [19]. The general public pilot sequence was replaced with a private pilot sequence that is randomly changed in each round of channel probing, so the combination of the channel and the random pilot sequence can be treated as a source of randomness for key generation. In [20], a scheme based on the cross multiplication of two-way randomness was proposed to further expand the volume of random resources. We note that a critical limitation is that the randomness from RP could be easily separated, thus eavesdroppers have a high probability to obtain the keys generated between legitimate nodes since the channel coefficients remain constant for a long time. To this end, we propose to address this limitation by mixing self-interference signals with random pilots at the eavesdropper, which realizes the security of key generation in static environments without resorting to multi-antenna transceivers or third-party nodes.

Second, wireless key generation protocols should be designed to support the ultra-reliable low-latency communications (URLLC) required for WNCS in IIoT applications. To the best knowledge of the authors, there is currently limited work considering low-latency key generation. In [22], optimal power and subcarrier allocation was theoretically analyzed to simultaneously generate keys and transmit data, but the process of exchanging side information extended the compressed air interface latency, making it difficult to meet the requirements of URLLC. Some works [23], [24] focused on reducing the complexity of algorithms deployed at transceivers to shorten the processing delay. However, the time consumption caused by standard procedures in wireless key generation including channel probing and information reconciliation results in lengthy transmission delays, which makes it unsuitable for URLLC implementations. Recently, the authors in [25] developed an un-identical key (UK)-based one-time pad (OTP) physical-layer secure transmission protocol which eliminated the information reconciliation in traditional identical key (IK)-based schemes by correcting key disagreements together with transmission errors. As such, both the processing overheads and communications latency were significantly reduced. Whereas, the standard interactions between the transceivers during channel probing is still time-consuming and it restricts existing wireless key generation protocols from meeting the URLLC requirements in IIoT. To minimize the transceiver interactions, we design a one-way encrypted transmission structure, so that the channel probing and secure transmission stages are completed simultaneously with the assistance of self-interference cancellation (SIC), which further shortens the air interface latency by more than half, and satisfies the URLLC requirements of key generation in WNCS.

Third, wireless key generation protocols for WNCS in IIoT should be robust to both passive and active attacks. The establishment of shared keys is based on the reciprocity of the uplink and downlink channels, which is only valid when the channel probing process is free from malicious interference. Therefore, most existing key generation schemes will suffer from high KDR when they experience active jamming attacks [26]. In [27], energy harvesting and channel hopping were considered as countermeasures to avoid the impact of the jammer. Similarly, a two-step secure and resilient transmission scheme was proposed in [28], where the keys generated from jammed channel observations were used as dynamic frequency hopping patterns to avoid hostile jamming. However, these frequency hopping-based schemes waste spectrum resources that could be used to serve massive IoT nodes. More recently, attack detection-based solutions were proposed to identify and neutralize active jamming attacks [29]. In [30], pilot contamination attacks in grant-free IoT networks were detected with high accuracy using a virtual channel representation and deep learning algorithm. Nevertheless, these solutions require multiple antennas at the access point/base station to protect uplink transmissions from active attacks, but do not consider downlink attacks on low-cost single-antenna IoT nodes. In our scheme, due to the loopback mechanism, even a single-antenna sensor can detect the presence of active attacks at the cost of a tiny delay without consuming additional frequency resources.

In this paper, we propose a novel key-based transmission protocol for secure low-latency encrypted communications in static wireless environments with attack detection for WNCS in IIoT applications. It not only addresses the above-mentioned three challenges, but also overcomes the limitations of applying standard key generation methods in WNCS networks. The main contributions are summarized as follows.

- We investigate the vulnerability of RP-based key generation schemes in static environments. We reveal that an eavesdropper could perform a two-step estimation process to obtain the random pilot information by leveraging the time-invariant channel property and thereby infer the legitimate channels due to leakage during the information reconciliation phase. The probability that an eavesdropper successfully deduces the legitimate key under different conditions is derived.
- We propose a one-way self-interference assisted en-

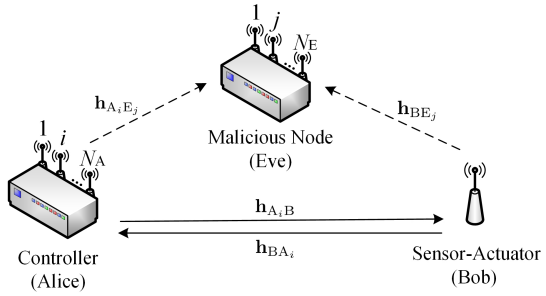


Fig. 1. System model of a WNCS with a sensor-actuator and a controller eavesdropped by a malicious node in a static IIoT environment.

crypted data transmission scheme, where artificial noise and SIC at the controller are used to conceal the randomness brought by the sensors. By employing this method, over-the-air interactions can be integrated to significantly decrease the transmission latency. Meanwhile, active attack detection is embedded in the protocol via the WNCS feedback loop, which is also effective and implementable for single antenna nodes.

- The security and performance advantages of our proposed scheme are theoretically analyzed and compared with the state-of-the-art IK-RP and UK-RP based approaches. Simulation results show that the proposed scheme outperforms these two benchmark approaches for a wide-range of system parameters. Moreover, the impact of different parameter selection is well investigated, which provides a guidance for its deployment and implementation.

The remainder of this paper is organized as follows. Section II provides the system and threat models and an overview of state-of-the-art key-based secure transmission protocols. Section III analyzes the vulnerability of RP-based key generation in static environments. The proposed one-way self-interference assisted encrypted data transmission scheme is illustrated in Section IV. In Section V, we provide a performance analysis, and the simulation results are discussed in Section VI. Conclusions are drawn in Section VII.

II. Model and Scheme Overview

A. System Model

As shown in Fig. 1, we consider a typical WNCS scenario, where a multi-antenna controller, Alice, and a low-cost single-antenna co-located sensor-actuator, Bob, need to securely exchange data over wireless channels, while a multi-antenna malicious node, Eve, attempts to acquire or disrupt the information transmitted between them via eavesdropping or active attacks. All nodes are assumed to be stationary or slow-moving and communicating in a static IIoT environment, which leads to infrequent variations in wireless channels. We consider block fading models, i.e., the channel coefficients remain constant during the long coherence interval. The communications between these nodes occur over an OFDM system with K subcarriers.

B. Threat Model

We consider two significant threats at the wireless physical layer which are passive eavesdropping and active attacks. For passive eavesdropping, Eve does not transmit signals to expose itself, and attempts to obtain useful information by observing and analyzing the data transmitted on public channels. We present a security analysis in Section III to show that the standard RP-based physical layer key generation scheme has a security vulnerability in static environments, making passive eavesdropping possible. For active attacks, we consider that Eve attempts to destroy the consistency of the keys generated in the uplink and downlink, so that legitimate nodes cannot decrypt correctly. Our proposed active attack detection based on a loopback mechanism is designed in Section IV. In the performance analysis and numerical simulation, both types of threats are considered to illustrate the security of the proposed scheme against active and passive threats.

C. RP-based Key Generation

The RP-based key generation schemes [18]–[20] were proposed recently to address the low KGR between two legitimate nodes in static environments. In this paper, we focus on two-way RP schemes [19], [20], but the subsequent analysis also applies to the one-way RP scheme [18]. The main procedures for the RP-based schemes are briefly explained as follows.

First, Alice selects a private pilot vector $\mathbf{s}$ of length K_s and Bob also selects a private pilot vector $\mathbf{v}$ of the same length, where each element of $\mathbf{s}$ and $\mathbf{v}$ is selected independently, randomly, and uniformly from a set of M symbols in a M-quadrature amplitude modulation (QAM) constellation. These two vectors (i.e., RP) are transmitted to each other through K_s uncorrelated subcarriers in adjacent time slots.

After the exchange of random pilots, Alice and Bob receives the following signals,

$$\mathbf{y}_{\mathrm{A}_i} = \mathbf{v} \circ \mathbf{h}_{\mathrm{BA}_i} + \mathbf{n}_\mathrm{A}, \tag{1}$$

$$\mathbf{y}_\mathrm{B} = \mathbf{s} \circ \mathbf{h}_{\mathrm{A}_i\mathrm{B}} + \mathbf{n}_\mathrm{B}, \tag{2}$$

respectively, where $\mathbf{h}_{\mathrm{A}_i\mathrm{B}}, \mathbf{h}_{\mathrm{BA}_i} \in \mathbb{C}^{K_\mathrm{s}\times 1}$ are the reciprocal channels between the ith antenna at Alice and Bob. The independent and identically distributed complex additive Gaussian noise terms at Alice and Bob are denoted by $\mathbf{n}_\mathrm{A}$ and $\mathbf{n}_\mathrm{B}$, respectively. By multiplying them with locally generated pilot vectors, the induced randomness from the other side can be extracted, and highly correlated random sequences $\mathbf{w}_{\mathrm{A}_i}$ and $\mathbf{w}_\mathrm{B}$ can be obtained at Alice and Bob, respectively, as

$$\mathbf{w}_{\mathrm{A}_i} = \mathbf{s} \circ \mathbf{v} \circ \mathbf{h}_{\mathrm{BA}_i} + \mathbf{v} \circ \mathbf{n}_\mathrm{A}, \tag{3}$$

$$\mathbf{w}_\mathrm{B} = \mathbf{s} \circ \mathbf{v} \circ \mathbf{h}_{\mathrm{A}_i\mathrm{B}} + \mathbf{s} \circ \mathbf{n}_\mathrm{B}, \tag{4}$$

where $\circ$ denotes the Hadamard product. Alice and Bob will thus have the common randomness, $\mathbf{s} \circ \mathbf{v} \circ \mathbf{h}_{\mathrm{A}_i\mathrm{B}}$.

Finally, by using quantization, information reconciliation, and privacy amplification, Alice and Bob can acquire identical keys generated based on their shared randomness. Repeating the above procedures, Alice and Bob can continuously generate keys even in a static environment, because the dynamic changes of the secret keys in this mechanism are determined by the randomly selected pilot vectors $\mathbf{s}$ and $\mathbf{v}$.

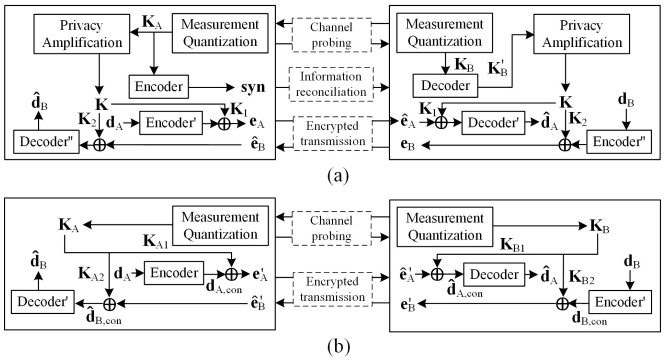


Fig. 2. Flow charts of two state-of-the-art OTP encrypted transmissions: (a) IK-based protocol (three phases) and (b) UK-based protocol (two phases).

D. OTP Encrypted Transmission

As illustrated in Fig. 2, two state-of-the-art OTP encrypted transmissions, namely IK-based and UK-based protocols [25], can be employed to realize secure communications when keys have been generated. Compared with the IK-based protocol, the UK-based protocol omits the information reconciliation phase in the key generation procedures and corrects the disagreements in keys and errors caused by the non-ideal channels at once, thereby simplifying the processing and improving the system transmission delay. The transmitted data $\mathbf{d}_{\mathrm{A}}$ and $\mathbf{d}_{\mathrm{B}}$ are encrypted and decrypted in an OTP fashion, where $\oplus$ denotes the bitwise XOR operator. In addition, these protocols were developed for low-latency communications by generating keys based on the instantaneous channel state information (CSI). Due to the limited randomness in WNCS, we further consider their use in static environments by combining them with RP-based key generation scheme into IK-RP and UK-RP, which serve as benchmarks for the comparison in Section V. For more details, please refer to [25].

III. Vulnerability of RP-based Key Generation Schemes in Static Environments

In this section, we explain the vulnerability of RP-based key generation schemes in static environments and analyze the probability of successful attacks at Eve. We assume that Eve is a powerful attacker who is capable to know the public protocol parameters including the symbol set, quantization levels, error-correcting code (ECC), etc. Indeed, the security of generated keys should not depend on the confidentiality of these parameters.

In each round, as the private pilot vectors $\mathbf{s}$ and $\mathbf{v}$ are randomly chosen and Eve has no information about the legitimate channel $\mathbf{h}_{\mathrm{A}_i\mathrm{B}}$, the secret keys generated by RP-based schemes should be secure enough to protect the information exchange [19]. However, in the following, we demonstrate that Eve with a strong computational capacity can infer the keys generated by Alice and Bob through observing the public transmissions and accelerate this process by launching active attacks. The two-step process required to obtain the legitimate keys is equivalent to obtaining the shared random sequences $\mathbf{w}_{\mathrm{A}_i}$ and $\mathbf{w}_{\mathrm{B}}$. Specifically, Eve needs to first estimate the private pilot vectors $\mathbf{s}$ and $\mathbf{v}$, then estimate the legitimate channel $\mathbf{h}_{\mathrm{A}_i\mathrm{B}}$.

Step 1: Estimation of $\mathbf{s}$ *and* $\mathbf{v}$

When Alice and Bob exchange the RP private vectors, the jth antenna of Eve receives

$$\mathbf{y}_{\mathrm{BE}_j} = \mathbf{v} \circ \mathbf{h}_{\mathrm{BE}_j} + \mathbf{n}_{\mathrm{E}}, \tag{5}$$

$$\mathbf{y}_{\mathrm{A}_i\mathrm{E}_j} = \mathbf{s} \circ \mathbf{h}_{\mathrm{A}_i\mathrm{E}_j} + \mathbf{n}_{\mathrm{E}}, \tag{6}$$

where $\mathbf{n}_{\mathrm{E}}$ denotes the noise at Eve. Note that as the subcarrier number and symbol set are known to Eve, the whole space of private vectors can be determined as a set of size $M^{K_{\mathrm{s}}}$ denoted by $\mathcal{P} = \{\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{M^{K_{\mathrm{s}}}}\}$. Eve can exploit this set $\mathcal{P}$ to construct an equal-size channel vector space $\mathcal{H} = \{\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{M^{K_{\mathrm{s}}}}\}$ by dividing the received signal $\mathbf{y}_{\mathrm{BE}_j}$ by each element in $\mathcal{P}$. Since $\mathbf{v}$ belongs to $\mathcal{P}$, the actual channel between Bob and Eve $\mathbf{h}_{\mathrm{BE}_j}$ must lie in $\mathcal{H}$ when the noise term is negligible. Moreover, due to the fixed positions of these nodes and the static wireless environment, all involved channel coefficients can be assumed to be constants. Based on this condition, the sets of candidate observations can be further calculated as

$$\mathcal{X}_n = \{\mathbf{h}_n \circ \mathbf{p}_1, \mathbf{h}_n \circ \mathbf{p}_2, \ldots, \mathbf{h}_n \circ \mathbf{p}_{M^{K_{\mathrm{s}}}}\},\ n = 1, \ldots, M^{K_{\mathrm{s}}}. \tag{7}$$

For the set corresponding to the actual $\mathbf{h}_{\mathrm{BE}_j}$, the following observations can always be found in this set. Therefore, as the number of cumulative observations increases, the uncertainty for $\mathbf{h}_{\mathrm{BE}_j}$ gradually decreases. To this end, Eve should find the distances between each observation $\mathbf{h}_{\mathrm{BE}_j}(t)$, where $t = 1, \ldots, T_1$, and all elements in the set $\mathcal{X}_n$, and then $\mathbf{h}_{\mathrm{BE}_j}$ can be statistically uniquely confirmed as

$$\hat{\mathbf{h}}_{\mathrm{BE}_j} = \arg\min_{\mathbf{h}_n \in \mathcal{H}} \sum_{t=1}^{T_1} \min(\|\mathbf{y}_{\mathrm{BE}_j}(t) - \mathbf{h}_n \circ \mathbf{p}_m\|_2), \tag{8}$$

where $\mathbf{p}_m \in \mathcal{P}$. $\|\cdot\|_2$ and $\min(\cdot)$ denote the Euclidean norm and the minimization operator, respectively. It is worth noting that a larger T_1 leads to a higher possibility to locate the actual $\hat{\mathbf{h}}_{\mathrm{BE}_j}$, and the minimum required rounds of observation increase when solving a protocol with larger M and K_{s} as shown in Fig. 3, which corresponds to a larger search space. Although this can postpone the key breach, it is still vulnerable to a long-term sniffing Eve. In addition, a higher signal-to-noise ratio (SNR) can accelerate Eve's access to the eavesdropping channel, and this condition is available for Eve to achieve by being located close to Alice and Bob.

Similarly, a reliable estimation of the actual $\hat{\mathbf{h}}_{\mathrm{A}_i\mathrm{E}_j}$ can also be obtained by Eve based on the observations of $\mathbf{y}_{\mathrm{A}_i\mathrm{E}_j}$. After estimations of both eavesdropping channels $\hat{\mathbf{h}}_{\mathrm{BE}_j}$ and $\hat{\mathbf{h}}_{\mathrm{A}_i\mathrm{E}_j}$ are known to Eve, the randomness induced by private pilot vectors disappears. The pilot vectors $\hat{\mathbf{s}}(t)$ and $\hat{\mathbf{v}}(t)$ sent by Alice and Bob can be estimated in each round as

$$\hat{\mathbf{s}}(t) = \arg\min_{\mathbf{p}_m \in \mathcal{P}} \|\mathbf{y}_{\mathrm{A}_i\mathrm{E}_j}(t) \oslash \hat{\mathbf{h}}_{\mathrm{A}_i\mathrm{E}_j} - \mathbf{p}_m\|_2, \tag{9}$$

$$\hat{\mathbf{v}}(t) = \arg\min_{\mathbf{p}_m \in \mathcal{P}} \|\mathbf{y}_{\mathrm{BE}_j}(t) \oslash \hat{\mathbf{h}}_{\mathrm{BE}_j} - \mathbf{p}_m\|_2, \tag{10}$$

where $t = T_1 + 1, \ldots, T_2$ and $\oslash$ is the Hadamard division.

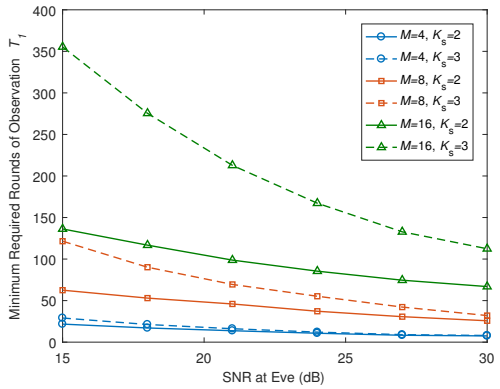


Fig. 3. The minimum required rounds of observation T_1 versus SNR at Eve under different modulation order M and number of uncorrelated subcarriers K_s.

According to [20], the theoretical KGR of a two-way random pilot scheme can be expressed as

$$R_\mathrm{tw} = \frac{1}{M_\mathrm{S}} I(\hat{\mathbf{h}}_{\mathrm{A}_i\mathrm{B}}; \hat{\mathbf{h}}_{\mathrm{BA}_i}) + \frac{M_\mathrm{A}}{M_\mathrm{S}} I(\mathbf{s}; \mathbf{y}_\mathrm{B} | \mathbf{y}_{\mathrm{A}_i\mathrm{E}_j}) + \frac{M_\mathrm{B}}{M_\mathrm{S}} I(\mathbf{v}; \mathbf{y}_{\mathrm{A}_i} | \mathbf{y}_{\mathrm{BE}_j}), \tag{11}$$

where $M_\mathrm{S} = M_\mathrm{A} + M_\mathrm{B}$ denotes the equivalent number of time slots within the coherence interval. M_A and M_B are the number of time slots allocated for Alice and Bob. In static environments, the values for M_S, M_A, and M_B can be set to an arbitrarily large number. As shown above, Eve can successfully estimate the random pilot vectors and thus the last two terms in (11) equals to zero. Moreover, due to the constant reciprocal channel estimations $\hat{\mathbf{h}}_{\mathrm{A}_i\mathrm{B}}$ and $\hat{\mathbf{h}}_{\mathrm{BA}_i}$, the first term on the right hand of (11) tends to be zero in static environments. Next, we further illustrate that the legitimate channel between Alice and Bob can also be inferred by Eve through long-term observation on the information reconciliation phase.

Step 2: Estimation of $\mathbf{h}_{\mathrm{A}_i\mathrm{B}}$

In most previous works, the legitimate channel $\mathbf{h}_{\mathrm{A}_i\mathrm{B}}$ is assumed to be uncorrelated with the eavesdropping channels when Eve is located more than half a wavelength away from Alice and Bob. Furthermore, they are considered to be independent of each other under the assumption that all channels follow the Gaussian distribution. However, this assumption has been challenged recently. Given the positions of transceivers, the CSI between them could be inferred with high accuracy at a third node by using machine-learning [31] or environmental reconstruction [32] methods. Meanwhile, since the legitimate channel is stationary and the reconciliation information is exchanged on public channels, the leaked information will also be accumulated by Eve for further amendment of $\mathbf{h}_{\mathrm{A}_i\mathrm{B}}$.

Without considering active attacks, the KDR is only affected by noise terms $\mathbf{n}_\mathrm{A}$ and $\mathbf{n}_\mathrm{B}$. We denote the raw keys generated after quantization in the tth round as $\mathbf{K}_{\mathrm{A},t}$ and $\mathbf{K}_{\mathrm{B},t}$, and the length of both of them is $L = K_\mathrm{s} \log_2 N_\mathrm{q}$, where N_q denotes the number of quantization levels. The KDR is expressed as

$$R_\mathrm{KD}(t) = \frac{\sum_{b=1}^{K_\mathrm{s}\log_2 N_\mathrm{q}} (\mathbf{K}_{\mathrm{A},t}(b) \oplus \mathbf{K}_{\mathrm{B},t}(b))}{K_\mathrm{s}\log_2 N_\mathrm{q}}. \tag{12}$$

Next, we show how active attacks from Eve accelerate this process. During the exchange of private pilot vectors, Eve could send another pilot vector $\mathbf{u}$ simultaneously. The signals received at Alice and Bob then become

$$\tilde{\mathbf{y}}_{\mathrm{A}_i} = \mathbf{v} \circ \mathbf{h}_{\mathrm{BA}_i} + \mathbf{u} \circ \mathbf{h}_{\mathrm{A}_i\mathrm{E}_j} + \mathbf{n}_\mathrm{A}, \tag{13}$$

$$\tilde{\mathbf{y}}_\mathrm{B} = \mathbf{s} \circ \mathbf{h}_{\mathrm{A}_i\mathrm{B}} + \mathbf{u} \circ \mathbf{h}_{\mathrm{BE}_j} + \mathbf{n}_\mathrm{B}, \tag{14}$$

respectively.

If active attacks are launched during the transmissions, the equivalent noise and R_KD will increase as the legitimate nodes do not know the pilot vector $\mathbf{u}$ Eve sends. Thus, more bits indicating inconsistent positions need to be exchanged in the information reconciliation phase. Based on Eve's estimation of the legitimate channel, $\hat{\mathbf{h}}_{\mathrm{A}_i\mathrm{B}}$, a pair of inferred keys $\hat{\mathbf{K}}_{\mathrm{A},t}$ and $\hat{\mathbf{K}}_{\mathrm{B},t}$ can be computed as

$$\hat{\mathbf{K}}_{\mathrm{A},t} = \hat{\mathbf{K}}_{\mathrm{B},t} = Q_u(\hat{\mathbf{s}}(t) \circ \hat{\mathbf{v}}(t) \circ \hat{\mathbf{h}}_{\mathrm{A}_i\mathrm{B}}), \tag{15}$$

where $t = T_1 + 1, \ldots, T_2$ and $Q_u(\cdot)$ denotes the quantization mapping function. We consider that Alice sends the positions of inconsistent bits to Bob so that he can reconcile $\mathbf{K}_{\mathrm{B},t}$ to be identical to $\mathbf{K}_{\mathrm{A},t}$. For simplicity, let us denote the proportion of keys leaked during the reconciliation as p_1, the initial KDR between $\hat{\mathbf{K}}_{\mathrm{A},t}$ and $\mathbf{K}_{\mathrm{A},t}$ as p_2, and $T = T_2 - T_1$. As such, the probability of Eve accurately estimating $\mathbf{h}_{\mathrm{A}_i\mathrm{B}}$ can be expressed as shown at the bottom of the next page.

Proof. See Appendix A. □

We note that $Q_u(\cdot)$ is a one-to-one bidirectional mapping, that is, when we have either the raw keys or the quantized values, the other can be obtained. Information reconciliation is mainly divided into two categories: grouping search protocols and ECC-based schemes, both of which will reveal several bits of $\mathbf{K}_{\mathrm{A},t}$ whether through the exchanged syndromes or the corrected symbols. Since this information is transmitted on public channels, it could be overheard and used by Eve to verify and modify her own key sequence $\hat{\mathbf{K}}_{\mathrm{A},t}$. We suppose that there are $p_2 L$ disagreement bits between Alice and Eve, which are caused by inaccurate channel estimation, and in each round of reconciliation an average of $p_1 L$ bits are exposed. Thus, the probability that all inconsistent bits have been corrected after T rounds is given by (16). Fig. 4 shows that this probability converges to one quickly, especially for a short length of key L, a larger p_1, and a smaller p_2, which validates that active attacks and accurate CSI inference are more harmful to RP-based schemes.

With the corrected key sequence $\hat{\mathbf{K}}'_{\mathrm{A},t}$, pilot vectors $\hat{\mathbf{s}}(t)$ and $\hat{\mathbf{v}}(t)$, the estimated channel $\hat{\mathbf{h}}_{\mathrm{A}_i\mathrm{B}}$ can be updated as

$$\hat{\mathbf{h}}'_{\mathrm{A}_i\mathrm{B}} = Q_u^{-1}(\hat{\mathbf{K}}'_{\mathrm{A},t}) \oslash \hat{\mathbf{s}}(t) \oslash \hat{\mathbf{v}}(t). \tag{17}$$

Through constant updates, this estimate gradually approaches the actual channel $\mathbf{h}_{\mathrm{A}_i\mathrm{B}}$. Thereafter, the randomness from both private pilot vectors and uncorrelated channels is eliminated, and all generated key bits can be deduced by Eve.

IV. Proposed One-way Self-interference Assisted OTP Encrypted Data Transmission

The vulnerability of the above RP-based secret key generation mainly comes from the long-term stable channels in static environments and frequent information exchanges, which also cause higher transmission latency and computational overhead. To solve these problems, we propose a one-way SI assisted OTP encrypted data transmission scheme to improve the security performance and transmission efficiency.

To provide perfect secrecy, we also consider using OTP to encrypt the uplink and downlink communications. Different from IK/UK-based schemes, we incorporate the key generation into the secure transmission process, and artificially change Eve's observed channels through the introduction of SI signals. As illustrated in Fig. 5, the uplink and downlink encrypted data transmission can be completed as follows, where A-X and B-X denote the Step X at Alice and Bob, respectively.

A. Uplink Transmission Stage

(B-1) Bob uses the random number generator to generate an OTP key $\mathbf{K}$, and divides it into three sub-keys $\mathbf{K}_1$, $\mathbf{K}_2$, and $\mathbf{K}_3$ according to the WNCS sensor data lengths and active attack verification requirement.

(B-2) The data collected by the sensor Bob $\mathbf{d}_\mathrm{B}$ with a length of L_B is encrypted through XOR-ing equal-length $\mathbf{K}_1$, and the ciphertext can be given as

$$\mathbf{e}''_\mathrm{B} = \mathbf{d}_\mathrm{B} \oplus \mathbf{K}_1. \tag{18}$$

Then, the confidential message $\mathbf{e}''_\mathrm{B}$ and the generated key $\mathbf{K}$ are concatenated and fed into an encoder, which outputs

$$\mathbf{e}_{\mathrm{B,con}} = E([\mathbf{e}''_\mathrm{B}, \mathbf{K}]), \tag{19}$$

where $E(\cdot)$ is the encoding function of a (C_1, n_1, k_1, t_1) ECC. The length of $\mathbf{e}_{\mathrm{B,con}}$ should be $L_{\mathrm{B,con}} = L_\mathrm{B} + L_\mathbf{K} + L_{\mathbf{syn}''}$, where $L_\mathbf{K}$ and $L_{\mathbf{syn}''}$ are the length of $\mathbf{K}$ and that of the syndrome $\mathbf{syn}''$ generated by $[\mathbf{e}''_\mathrm{B}, \mathbf{K}]$, respectively.

(A-1) Alice generates a random sequence $\mathbf{SI}$ of $L_\mathbf{SI}$ length as self-interference, which is also sent to the SIC[1] module.

(B-3&A-2) Bob sends the uplink signal $\mathbf{e}_{\mathrm{B,con}}$ simultaneously with Alice's $N_{\mathrm{A_T}}$ transmit antennas sending the artificial noise self-interference signal $\mathbf{SI}$. The signals are superimposed on public channels and received at the $N_{\mathrm{A_R}}$ receive antennas of Alice ($N_{\mathrm{A_T}} + N_{\mathrm{A_R}} = N_\mathrm{A}$) as

$$\mathbf{y}_{\mathrm{A}_{i_\mathrm{R}}} = \mathbf{e}_{\mathrm{B,con}} \circ \mathbf{h}_{\mathrm{BA}_{i_\mathrm{R}}} + \mathbf{SI} \circ \mathbf{h}_{\mathrm{A}_{i_\mathrm{T}}\mathrm{A}_{i_\mathrm{R}}} + \mathbf{n}_\mathrm{A}, \tag{20}$$

[1]Specific SIC algorithms and hardware implementations are beyond the scope of this paper. More details can be found in [33]. We also note that although SIC introduces additional signal processing, it is a low-complexity algorithm implemented in hardware, and its time consumption is negligible relative to the air interface latency.

where $\mathbf{h}_{\mathrm{A}_{i_\mathrm{T}}\mathrm{A}_{i_\mathrm{R}}}$ is the self-interference channel from the i_Tth transmit antenna to the i_Rth receive antenna. Here, we assume all relevant constant channels have been measured aforehand and pre-stored at Alice and Bob.

(A-3) Since $\mathbf{SI}$ and static channels are available at Alice, the SI term in (20) can be subtracted and a noisy version of $\mathbf{e}_{\mathrm{B,con}}$ can be obtained. Subsequently, the encrypted message and the whole key can be recovered as

$$[\hat{\mathbf{e}}''_\mathrm{B}, \hat{\mathbf{K}}] = D(\hat{\mathbf{e}}_{\mathrm{B,con}}) = [\mathbf{e}''_\mathrm{B}, \mathbf{K}], \tag{21}$$

where $D(\cdot)$ is the decoding function of (C_1, n_1, k_1, t_1). The second equation in (21) holds when the error ratio is within the correcting capability of the ECC.

(A-4) Alice decomposes the recovered key $\hat{\mathbf{K}}$ into $\hat{\mathbf{K}}_1$, $\hat{\mathbf{K}}_2$, and $\hat{\mathbf{K}}_3$, and decrypts $\hat{\mathbf{e}}''_\mathrm{B}$ to plaintext as

$$\hat{\mathbf{d}}_\mathrm{B} = \hat{\mathbf{e}}''_\mathrm{B} \oplus \hat{\mathbf{K}}_1 = \mathbf{e}''_\mathrm{B} \oplus \mathbf{K}_1 = \mathbf{d}_\mathrm{B}. \tag{22}$$

B. Downlink Transmission Stage

(A-5) In the downlink from Alice to Bob, $\hat{\mathbf{K}}_2$ is used to encrypt the WNCS control data $\mathbf{d}_\mathrm{A}$ of L_A length through XOR operation as

$$\mathbf{e}''_\mathrm{A} = \mathbf{d}_\mathrm{A} \oplus \hat{\mathbf{K}}_2. \tag{23}$$

Next, the encrypted message $\mathbf{e}''_\mathrm{A}$ is input to an encoder, and the encoded data is concatenated with $\hat{\mathbf{K}}_3$ as

$$\mathbf{e}_{\mathrm{A,con}} = [E'(\mathbf{e}''_\mathrm{A}), \hat{\mathbf{K}}_3], \tag{24}$$

where $E'(\cdot)$ is the encoding function of a (C_2, n_2, k_2, t_2) ECC. As $\hat{\mathbf{K}}_3$ is used to verify the existence of active attacks rather than encryption, no encoding is required.

(A-6) The ciphertext $\mathbf{e}_{\mathrm{A,con}}$ of $L_{\mathrm{A,con}} = L_\mathrm{A} + L_3 + L^{(2)}_{\mathbf{syn}''}$ length is transmitted to Bob over public channels, where L_3 and $L^{(2)}_{\mathbf{syn}''}$ are the length of $\mathbf{K}_3$ and that of the syndrome generated by $\mathbf{e}''_\mathrm{A}$, respectively.

(B-4) Once $\hat{\mathbf{e}}_{\mathrm{A,con}}$ is received at Bob, the sub-key $\hat{\mathbf{K}}'_3$ used for attack detection is extracted and compared with the locally generated $\mathbf{K}_3$. If the noise power exceeds the preset empirical threshold θ_th, i.e.,

$$\mathbb{E}\{\|\hat{\mathbf{K}}'_3 - \mathbf{K}_3\|_2^2\} \geq \theta_\mathrm{th}, \tag{25}$$

where $\mathbb{E}\{\cdot\}$ represents the expectation operation, the encrypted control information of this round is ignored and the potential threat is reported to the controller. Note that the interleaver and de-interleaver can be employed in practical implementations to prevent Eve from launching burst active attacks on the $E'(\mathbf{e}''_\mathrm{A})$ corresponding part of $\mathbf{e}_{\mathrm{A,con}}$.

(B-5) When no attack is detected, the control message $\mathbf{d}_\mathrm{A}$ can be decrypted and corrected as

$$\hat{\mathbf{d}}_\mathrm{A} = D'(\hat{\mathbf{e}}''_\mathrm{A} \oplus \mathbf{K}_2) = \mathbf{e}''_\mathrm{A} \oplus \mathbf{K}_2 = \mathbf{d}_\mathrm{A}, \tag{26}$$

$$P = 1 - \sum_{i=1}^{p_2 L-1} \left\{ \frac{p_2 L!}{i!(p_2 L - i)!} \left(\frac{(L-i)![(1-p_1)L]!}{L![(1-p_1)L - i]!} \right)^T - \sum_{j=0}^{p_2 L - i - 1} \frac{(p_2 L - i)!}{j!(p_2 L - i - j)!} \left(\frac{[(1-p_1)L]![(1-p_2)L + j]!}{L![(1-p_1-p_2)L + j]!} \right)^T \right\} - \left(\frac{[(1-p_1)L]![(1-p_2)L]!}{L![(1-p_1-p_2)L]!} \right)^T. \tag{16}$$

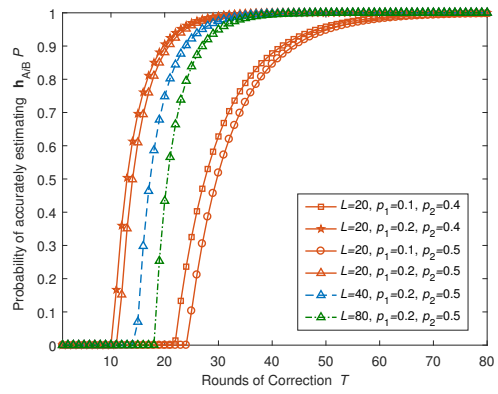


Fig. 4. Probability of Eve accurately estimating $\mathbf{h}_{\mathrm{A}_i\mathrm{B}}$ versus rounds of correction T under different length of key L, leakage proportion during the information conciliation p_1, and initial KDR between Alice and Eve p_2.

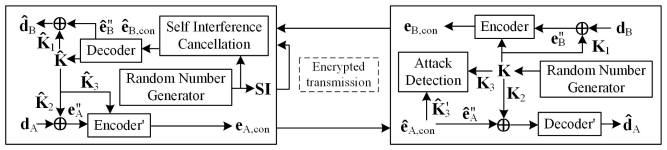


Fig. 5. Flow chart of the proposed one-way self-interference assisted OTP encrypted data transmission (only one phase).

where $D'(\cdot)$ is the decoding function of (C_2, n_2, k_2, t_2).

V. Performance Analysis

In this section, we evaluate the performance of the proposed scheme by comparing it with existing mechanisms IK-RP and UK-RP in terms of communication latency, secure transmission rate, successful eavesdropping probability, and attack detection accuracy.

A. Communication Latency

In Fig. 5, we see that the requisite number of interactions is reduced to one, compared to three (two) in IK-RP (UK-RP). Similar to [25], we only consider the air interface latency between Alice and Bob in one round trip. The latencies required for these schemes to achieve OTP secure transmission are

$$T_{\text{latency}}^{\text{IK-RP}} = \frac{2}{B}\left\lceil \frac{L_{\text{A}}+L_{\text{B}}+L_{\mathbf{syn}}}{L}+\frac{L_0}{K_{\text{s}}}\right\rceil+\frac{1}{B}\left(\left\lceil \frac{L_{\mathbf{syn}}+L_0}{K}\right\rceil + \left\lceil \frac{L_{\text{A}}+L_{\mathbf{syn}}^{(1)}+L_0}{K}\right\rceil+\left\lceil \frac{L_{\text{B}}+L_{\mathbf{syn}}^{(2)}+L_0}{K}\right\rceil\right)+\frac{5d}{c}, \tag{27}$$

$$T_{\text{latency}}^{\text{UK-RP}} = \frac{2}{B}\left\lceil \frac{L_{\text{A}}+L_{\text{B}}+L_{\mathbf{syn}'}}{L}+\frac{L_0}{K_{\text{s}}}\right\rceil+\frac{4d}{c} + \frac{1}{B}\left(\left\lceil \frac{L_{\text{A}}+L_{\mathbf{syn}'}^{(1)}+L_0}{K}\right\rceil+\left\lceil \frac{L_{\text{B}}+L_{\mathbf{syn}'}^{(2)}+L_0}{K}\right\rceil\right), \tag{28}$$

and

$$T_{\text{latency}}^{\text{proposed}} = \frac{1}{B}\left(\left\lceil \frac{L_{\text{A,con}}+L_0}{K}\right\rceil+\left\lceil \frac{L_{\text{B,con}}+L_0}{K}\right\rceil\right)+\frac{2d}{c}, \tag{29}$$

respectively, where $\lceil\cdot\rceil$ denotes the ceiling function. B, L_0, K, d, and c are the bandwidth of each subcarrier, the indispensable overhead (e.g., the synchronization header, PHY header and frame payload), the number of subcarriers, the average transmission distance between Alice and Bob, and the speed of light, respectively. Based on the above, we have

$$T_{\text{latency}}^{\text{proposed}} < T_{\text{latency}}^{\text{UK-RP}} < T_{\text{latency}}^{\text{IK-RP}}, \tag{30}$$

which shows that our proposed solution achieves a significantly lower communication latency compared with existing schemes.

Proof. See Appendix B. □

B. Secure Transmission Rate

The secure transmission rate is the number of data bits securely transmitted per unit time. The upper bounds of the secure transmission rate of IK-RP and UK-RP schemes [25] can be expressed as

$$R_{\text{UB}}^{\text{IK-RP}} = \frac{(L_{\text{A}}+L_{\text{B}})(1-4\epsilon)-2}{(1-2\epsilon)T_{\text{latency}}^{\text{IK-RP}}}, \tag{31}$$

$$R_{\text{UB}}^{\text{UK-RP}} = \frac{(1+\rho)(L_{\text{A}}+L_{\text{B}})(1-2\epsilon)-2}{T_{\text{latency}}^{\text{UK-RP}}}, \tag{32}$$

where ϵ denotes the error ratio in transmissions and ρ denotes the redundancy coefficient which is expressed by the bit ratio of the employed ECC syndrome to the encoded sequence.

In our proposed scheme, the input of the uplink decoder is the result of SIC, which can be regarded as a cascaded of two channels. Hence, the equivalent error ratio is given as

$$\epsilon_{\text{eq}} = \epsilon_0 + \epsilon - 2\epsilon_0\epsilon, \tag{33}$$

where ϵ_0 is the error ratio caused by imperfect SIC. In the downlink transmission, the transmission rate is similar to the UK-RP scheme. Therefore, the upper bound of the secure transmission rate of the proposed scheme can be given by

$$R_{\text{UB}}^{\text{proposed}} = \frac{1}{T_{\text{latency}}^{\text{proposed}}}\left[L_{\text{A}}+L_{\text{B}}-2\alpha\epsilon_{\text{eq}}(1+\rho)(2L_{\text{B}}+L_{\text{A}}) -2\epsilon(1+\rho)L_{\text{A}}-2\right]. \tag{34}$$

where $\alpha = 1-\mathbb{E}\{\varepsilon_{\text{E}}\}$ is the information leakage ratio to Eve and $\mathbb{E}\{\varepsilon_{\text{E}}\}$ is the average block error rate (BLER) at Eve which will be further discussed in subsection V-D.

Proof. See Appendix C. □

C. Passive Eavesdropping Probability

In order to ensure that the encrypted information and the shared keys are protected from Eve and can be recovered by Alice, the SI signal is injected at the receiving end simultaneously during the encrypted data transmission, and the original encrypted information can be restored via the SIC technique as discussed in Section IV. Due to the imperfections in transceiver operations, completely cancelling SI is impossible

and residuals will remain [34], [35]. Therefore, the received signal at Alice after SI cancellation can be expressed as

$$\mathbf{y}_{\mathrm{A}_{i_{\mathrm{R}}}} = \mathbf{e}_{\mathrm{B,con}} \circ \mathbf{h}_{\mathrm{BA}_{i_{\mathrm{R}}}} + \mathbf{RSI} + \mathbf{n}_{\mathrm{A}}, \tag{35}$$

where $\mathbf{e}_{\mathrm{B,con}} \sim \mathcal{CN}(0, P_{\mathrm{B}}\mathbf{I})$, $\mathbf{h}_{\mathrm{BA}_{i_{\mathrm{R}}}} \sim \mathcal{CN}(0, \sigma^2_{h_{\mathrm{AB}}}\mathbf{I})$, $\mathbf{n}_{\mathrm{A}} \sim \mathcal{CN}(0, \sigma_n^2\mathbf{I})$. Furthermore, P_{A}, $\sigma^2_{h_{\mathrm{AB}}}$, σ_n^2 and $\mathbf{I}$ are the transmit power at Bob, the average power of each element of $\mathbf{h}_{\mathrm{BA}_{i_{\mathrm{R}}}}$, the noise power, and the identity matrix, respectively. $\mathbf{RSI} \sim \mathcal{CN}(0, \beta P_{\mathrm{A}}\sigma^2_{h_{\mathrm{AA}}}\mathbf{I})$ represents the residual SI (RSI), where β, P_{A}, and $\sigma^2_{h_{\mathrm{AA}}}$ are the strength of RSI compared to the desired received signal, the transmit power at Alice, and the average power of each element of $\mathbf{h}_{\mathrm{A}_{i_{\mathrm{T}}}\mathrm{A}_{i_{\mathrm{R}}}}$, respectively. As such, the equivalent signal-to-interference-plus-noise ratio (SINR) at Alice can be given as

$$\gamma_{\mathrm{A}} = \frac{P_{\mathrm{B}}\sigma^2_{h_{\mathrm{AB}}}}{\beta P_{\mathrm{A}}\sigma^2_{h_{\mathrm{AA}}} + \sigma_n^2}. \tag{36}$$

Similarly, the received signal at Eve can be expressed as

$$\mathbf{y}_{\mathrm{E}_j} = \mathbf{e}_{\mathrm{B,con}} \circ \mathbf{h}_{\mathrm{BE}_j} + \mathbf{SI} \circ \mathbf{h}_{\mathrm{A}_{i_{\mathrm{T}}}\mathrm{E}_j} + \mathbf{n}_{\mathrm{E}}. \tag{37}$$

As the SI signal is randomly generated and unknown to Eve, the SINR at Eve is given as

$$\gamma_{\mathrm{E}} = \frac{P_{\mathrm{B}}\sigma^2_{h_{\mathrm{BE}}}}{P_{\mathrm{A}}\sigma^2_{h_{\mathrm{AE}}} + \sigma_n^2}, \tag{38}$$

where $\sigma^2_{h_{\mathrm{BE}}}$ and $\sigma^2_{h_{\mathrm{AE}}}$ are the average power of each element of $\mathbf{h}_{\mathrm{BE}_j}$ and that of $\mathbf{h}_{\mathrm{A}_{i_{\mathrm{T}}}\mathrm{E}_j}$. We also note that since the SI signal and the transmitted signal are superimposed at Eve, and the SI signal changes in each round, Eve cannot separate it from receiving signals in a similar way as in Section III. To meet the needs of URLLC, we consider using ECC with a finite blocklength for error correction, therefore the mutual information which is commonly used to evaluate the security performance will be inaccurate. Here, we exploit the results about well-known PPV bound [36] to analyze the relationship between the code rate k/n, SINR γ, and BLER ε. According to [38, (298)], we have

$$C - \sqrt{\frac{V}{n}}Q^{-1}(\varepsilon) + \frac{1}{2n}\log_2 n = \frac{k}{n}, \tag{39}$$

where $C = \frac{1}{2}\log(1+\gamma)$ and $V = \frac{\gamma}{2}\frac{\gamma+2}{(\gamma+1)^2}\log_2^2 e$. For a finite blocklength n, the reliability and security requirements can be represented by [37]

$$\mathbb{E}\{\varepsilon_{\mathrm{A}}\} \leq \beta_1, \mathbb{E}\{\varepsilon_{\mathrm{E}}\} \geq \beta_2, \tag{40}$$

where β_1 and β_2 denote the maximum allowable average BLER at Alice and the minimum allowable average BLER at Eve, respectively. Given the blocklength and code rate, ε_{B} and ε_{E} can be obtained by substituting (36) and (38) into (39), respectively. In this paper, we predefine β_1, and use $\mathbb{E}\{\varepsilon_{\mathrm{E}}\}$ as the security metric to evaluate the performance of our proposed scheme under different system parameters.

D. Active Attack Detection Accuracy

Since the information loopback and preset empirical threshold are proposed to identify active attacks, there will always be some misjudgements. To simplify our analysis, we define the attack detection accuracy as [30]

$$P' = 1 - (p_{\mathrm{MD}} + p_{\mathrm{FA}}), \tag{41}$$

where p_{MD} and p_{FA} denote the miss detection rate (there is an active attack but it has not been successfully identified) and the false alarm rate (there is no attack but an attack is reported), respectively. Therefore, a higher accuracy P' indicates a better attack detection performance.

We note that both the power of active attacks P_{E} and the selection of the preset empirical threshold θ_{th} impact on P'. If θ_{th} is small, it is possible to misjudge the distortion caused by noise at the receiver as an attack and thus increase p_{FA}. In contrast, attacks with relatively low P_{E} will be missed when θ_{th} is selected large. Moreover, the detection accuracy P' is also affected by L_3, since the expectation is performed with respect to (w.r.t.) L_3 bits, where an insufficient L_3 cannot provide a reliable statistical estimate while a significantly large L_3 in turn reduces the secure transmission rate.

VI. Simulation Results and Discussion

In this section, we first show the performance advantages of our proposed one-way self-interference assisted encrypted data transmission scheme compared with existing schemes. Then, the impacts of different system parameters are evaluated and the parameter selection criteria are discussed.

A. Simulation Setup

As shown in Fig. 6, we consider a practical factory warehouse scenario modeled using a commercial ray-tracing software, Wireless InSite [38], which provides high accuracy in simulating practical wireless channels [39], [40]. The size of this study area is about 40.2 m × 78.5 m × 20.8 m. In this factory environment, 21 single-antenna sensors-actuators (Bob) shown as green blocks in Fig. 6 which are fixed on robots and shelves located 2 m above the ground and first floor, and on the forklift and container lift located 1 m above the ground and first floor. They are all controlled by a six-antenna controller (Alice) with antennas shown as blue blocks located 0.5 m above the first floor. Alice uses three antennas for transmitting SI signals in the uplink transmission stage and another three antennas for receiving the superposition of the desired signal from Bob and SI signals. Then, SIC is executed to retrieve the desired signal as described in Section IV. During uplink transmissions, 471 potential eavesdropper locations shown as red blocks located 1.2 m above all accessible floors and uniformly separated by 2 m are considered for Eve attempting to obtain useful information through overhearing the public transmissions. All antennas are omnidirectional with vertical polarization. Other simulation parameters are summarized in Table I, if not specifically mentioned.

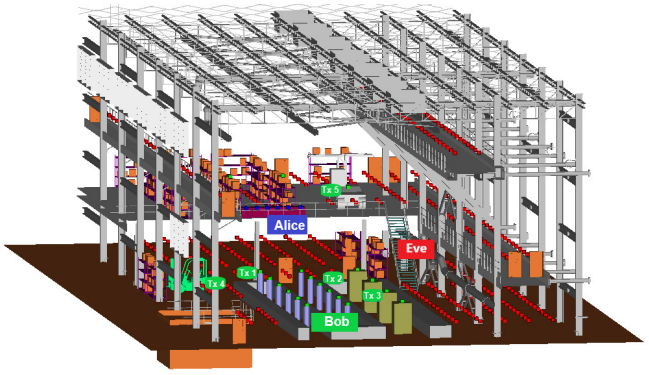


Fig. 6. Ray-tracing based factory scenario model, in which the blue, green, and red blocks denote locations for Alice, Bob, and Eve, respectively.

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Carrier frequency, f_c	1 GHz
Number of subcarriers, K	16
Bandwidth, B	2 MHz
Indispensable overhead, L_0	11 bytes
Transmit power, P_B	10 dBm
Length of $\mathbf{K}_3$, L_3	50 bits
Number of quantization levels, N_q	2
Error ratios, ϵ and ϵ_0	0.1
Information leakage ratio, α	0.1
Redundancy coefficient, ρ	0.5

B. Results and Discussion

In the practical IIoT scenario, we need to ensure that the proposed scheme satisfies the functional and security requirements. Specifically, the communication should satisfy the requirements of URLLC, that is, two-way data transmission should be completed within 1 ms, and the decoding accuracy at legitimate nodes should be higher than 99.999% [41]. At the same time, the system is protected from both active and passive threats, which means that useful information leaked to Eve should be minimized while active attack detection accuracy should be maximized.

Fig. 7 plots the communication latency using our proposed scheme compared with two existing key generation schemes [19], [25]. As analyzed previously, the proposed scheme reduces the air interface latency by more than half by simplifying the interaction and applying SI signals. Meanwhile, we see that latency increases almost linearly with the length of the data to be transmitted for all schemes, and the larger redundancy coefficient ρ also slightly increases the communication latency. Moreover, the proposed approach can meet the URLLC air interface round-trip latency requirement of 1 ms (denoted by the dashed line) even if data length reaches 5,000 bits, while IK-RP and UK-RP solutions can only support a maximum data length of fewer than 2,000 bits. This indicates that our scheme has a wider range of application scenarios, such as high-precision control with a large amount of transmitted data.

Fig. 8 depicts the comparison of secure transmission rate for different schemes, in which our proposed scheme outperforms the two benchmarks mainly due to the short key

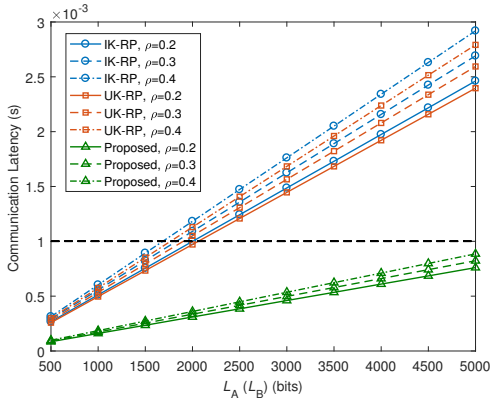


Fig. 7. Comparison of communication latency between different schemes for different data length $L_A(L_B)$ and redundancy coefficient ρ. The dashed line indicates the URLLC requirement.

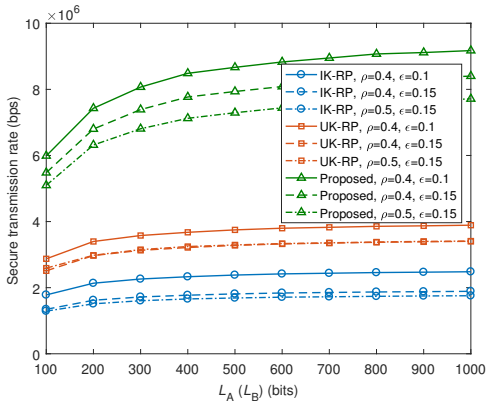


Fig. 8. Comparison of secure transmission rate between different schemes for different redundancy coefficient ρ and error ratio in transmissions ϵ.

generation time. Besides, it is observed that the transmission rate increases with the data length and gradually flattens out, because the proportion of fixed overhead L_0 in the entire data block becomes negligible. We also show the impact of the redundancy coefficient ρ and error ratio ϵ. When the channel quality is poor, i.e., ϵ is high, more redundancy is generally required to correct all errors, thereby compromising the secure transmission rate. Moreover, on the premise that all errors can be corrected, further increasing the redundancy ratio ρ will also reduce efficiency, which should be avoided.

The effects of the SIC error ratio ϵ_0, length of $\mathbf{K}_3$ L_3, and information leakage ratio α on the secure transmission rate of the proposed scheme are illustrated in Fig. 9. We see that decreasing the ϵ_0 or α results in an increasing secure transmission rate, which implies that both a more effective SIC algorithm and a lower leakage are beneficial to the system security. We note that these two factors are interrelated. Alice needs to transmit the SI signals with a higher power to conceal the useful information, and thus reducing the leakage to Eve, but this requires a stronger SIC module to eliminate the undesired impact on her own channel observations. Similarly, the secure transmission rate can also be enhanced by shortening L_3, whereas this will weaken the capability of Alice and Bob

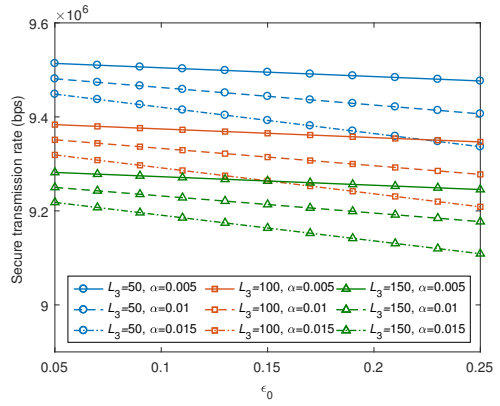


Fig. 9. The impact of error ratio of SIC ϵ_0, length of $\mathbf{K}_3$ L_3, and information leakage ratio α on secure transmission rate of the proposed scheme.

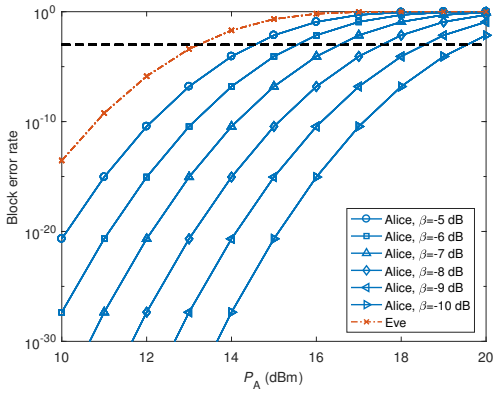


Fig. 11. Block error rate ε versus transmit power of SI signal P_{A} and RSI strength β when code rate $k/n = 0.9$ for Tx 1. The dashed line indicates the URLLC requirement.

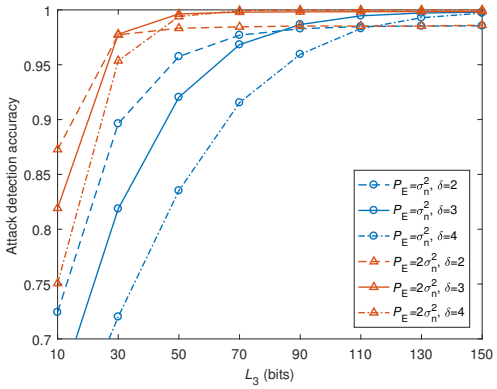


Fig. 10. Attack detection accuracy as a function of the length of $\mathbf{K}_3$ L_3, received active attack power P_{E}, and threshold parameter δ.

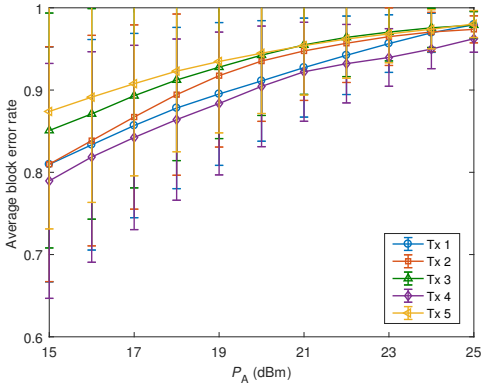


Fig. 12. Average block error rate at Eve $\mathbb{E}\{\varepsilon_{\mathrm{E}}\}$ versus transmit power of SI signal P_{A} for different Tx positions.

to accurately recognize active attacks as shown in Fig. 10.

In Fig. 10, we can see that for active attacks, the attack detection accuracy P' increases rapidly with L_3 and approaches 1 under various parameters. This indicates that L_3 can be set to a reasonably small value which also corresponds to a high secure transmission rate. For instance, when $P_{\mathrm{E}} = 2\sigma_n^2$ and $\delta = 3$, L_3 of 70 bits is enough to provide an accurate identification. Furthermore, active attacks with higher power are easier to be identified. Specifically, detection accuracy for attack signals with power P_{E} twice the noise power σ_n^2 is always higher than that for attack signals with the same power as the noise. We also observe a tradeoff in selecting the threshold $\theta_{\mathrm{th}} = \mu + \delta\sigma^2$, where μ and σ^2 denote the mean and variance of $\mathbf{K}_3$, respectively. Under the given conditions, the threshold with $\delta = 3$ outperforms the other two cases when sufficient L_3 is provided, because a smaller θ_{th} may enhance p_{FA} while a larger θ_{th} may contribute to increasing p_{MD} as discussed in Section V-D. Therefore, δ should be carefully selected to achieve a better attack detection accuracy.

Fig. 11 illustrates the BLERs of Eve and Alice with different RSI strength β to show the security of the proposed scheme. In this figure, we consider Tx 1 in Fig. 6 and the location of Eve with the highest SINR. Firstly, it shows that increasing P_{A} will increase the BLER of Alice and Eve at the same time, but due to the SIC capability, Alice can always achieve a higher SINR, and thus has a lower BLER than Eve. We notice that a smaller β, i.e., a more powerful SIC module, can easily achieve both reliability and security requirements in (40). For instance, $P_{\mathrm{A}} = 19$ dBm and $\beta = -10$ dB can ensure that the BLER of Alice satisfies the 99.999% system reliability for URLLC (denoted by the dashed line), while the BLER of Eve quickly approaches 1. According to [34], β is typically [-100, -45] dB, which is sufficient to satisfy URLLC requirements.

In Fig. 12, we show the average BLER at Eve for Bob located at different positions (Tx 1–Tx 5 as shown in Fig. 6). As P_{A} increases, $\mathbb{E}\{\varepsilon_{\mathrm{E}}\}$ increases for all cases, which verifies that the analysis of Fig. 11 in the previous paragraph is also applicable to other legitimate nodes. Moreover, the variance decreases with the increase of P_{A}. This means P_{A} should be relatively large to ensure that the system is secure and robust to widely distributed eavesdroppers. We can find that the gaps between these curves are not significant for the five nodes with different distances randomly selected on the ground and first floors, which shows that the proposed scheme can protect any legitimate node in the given area from passive eavesdropping.

Fig. 13 explores the impact of different coding parameters on security performance. For a fixed blocklength n, $\mathbb{E}\{\varepsilon_{\mathrm{E}}\}$

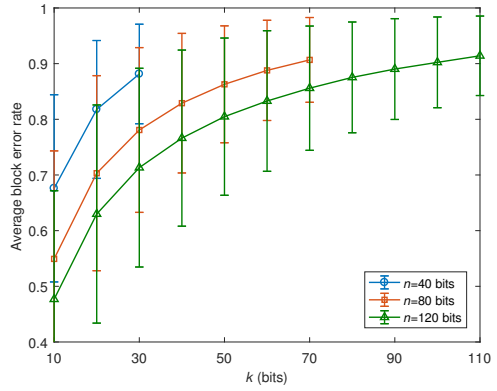


Fig. 13. Average block error rate at Eve $\mathbb{E}\{\varepsilon_{\rm E}\}$ as a function of different blocklengths n and message lengths k (code rates n/k) for Tx 1.

increases with the message length k. This is because a large k implies fewer syndromes, and thus the leakage can be reduced accordingly. We also note that the selected code rate k/n should satisfy the requirement of error correction at the controller. In addition, for the same code rate, the length of n only slightly improves $\mathbb{E}\{\varepsilon_{\rm E}\}$, which indicates that short codes introducing shorter latency can also satisfy the security requirements.

VII. Conclusions

In this paper, we designed a low-latency wireless key generation protocol for secure transmission in static IIoT environments. Firstly, we identified the vulnerability of existing RP-based key generation schemes in static environments. We found that the randomness contained in the generated keys could be compromised with a high probability by an eavesdropper who eavesdrops on the public information exchanges over a long time period. A key cracking method based on private pilots and legitimate channels estimations and its probability of success were presented. To avoid such eavesdropping, we proposed a one-way SI assisted OTP encrypted data transmission scheme, which addresses the problem of generating secret keys in static environments by introducing artificial noise and SIC technology. The proposed scheme also shortened the air interface latency through simplified interaction, and prevented active attacks through loopback verification, which satisfied both URLLC and security requirements for WNCS scenarios in IIoT. Performance analysis was provided to highlight the advantages of our proposed scheme over other benchmarks in terms of communication latency and secure transmission rate, and the robustness of our scheme to eavesdropping and active attacks. Numerical simulations verified the correctness of our analysis and illustrated the impacts of a wide range of system parameters on the security performance.

Appendix A
Proof of Equation (16)

Assume that the number of initial disagreement bits between the keys generated at Alice and Eve is p_2L and the average number of bits leaked in each round of reconciliation is p_1L. Since the inconsistency between $\mathbf{K}_{{\rm A},t}$ and $\mathbf{K}_{{\rm B},t}$ is caused by noise, the positions leaked in each round is random. Therefore, the probability that Eve can correct all inconsistent bits after T rounds is equal to the probability that all p_2L positions of error bits have been traversed, where p_1L positions in the key of L-bit length are randomly exposed in each round.

Firstly, we consider the inverse-event. The total number of possible incidents of leakage after T rounds of reconciliation is $N_{\rm all}=\binom{L}{p_1L}^T$, where $\binom{x}{y}$ indicates the number of combinations that randomly select y from x. In all these incidents, we need to exclude the incidents that specific p_2L positions have not been completely traversed, whose number can be given as

$$\begin{aligned} N_{\rm ex}=&\sum\nolimits_{i=1}^{p_2L-1}\left[\binom{p_2L}{i}\binom{L-i}{p_1L}^T\right.\\ &\left.-\sum\nolimits_{j=0}^{p_2L-i-1}\binom{p_2L-i}{j}\binom{(1-p_2)L+j}{p_1L}^T\right]\\ &+\binom{(1-p_2)L}{p_1L}^T. \end{aligned} \tag{42}$$

Thus, the target probability can be calculated as

$$P=1-\frac{N_{\rm ex}}{N_{\rm all}}. \tag{43}$$

By substituting (42) and applying the binomial coefficient $\binom{x}{y}=x!/[y!(x-y)!]$ into (43), the expression in (16) can be derived. This completes the proof.

Appendix B
Proof of Inequations (30)

We assume that the same code rate is used in all involved ECCs. For a ECC (C',n',k',t'), we define the redundancy coefficient as $\rho=(n'-k')/k'$. Thus, we have $L^{(1)}_{\mathbf{syn}}=L^{(1)}_{\mathbf{syn}'}=\rho L_{\rm B}$, $L^{(2)}_{\mathbf{syn}}=L^{(2)}_{\mathbf{syn}'}=\rho L_{\rm A}$, and $L_{\mathbf{syn}}=L_{\mathbf{syn}'}=\rho(L_{\rm A}+L_{\rm B})$. From equations (27) and (28), it is easy to decide their relation as $T^{\rm UK-RP}_{\rm latency}<T^{\rm IK-RP}_{\rm latency}$. Then, we demonstrate that $T^{\rm proposed}_{\rm latency}<T^{\rm UK-RP}_{\rm latency}$ in the following. Similarly, $L_{\rm B,con}$ and $L_{\rm A,con}$ in (29) can be given as

$$L_{\rm B,con}=L_{\rm B}+L_{\mathbf{K}}+L_{\mathbf{syn}''}=(1+\rho)(2L_{\rm B}+L_{\rm A}+L_3), \tag{44}$$

$$L_{\rm A,con}=L_{\rm A}+L_3+L^{(2)}_{\mathbf{syn}''}=(1+\rho)(L_{\rm A}+L_3). \tag{45}$$

When $\lceil x\rceil$ is approximated to x, $T^{\rm proposed}_{\rm latency}$ is rewritten as

$$T^{\rm proposed}_{\rm latency}=\frac{2(1+\rho)(L_{\rm A}+L_{\rm B}+L_3)+2L_0}{BK}+\frac{2d}{c}, \tag{46}$$

and $T^{\rm UK-RP}_{\rm latency}$ is given as

$$\begin{aligned} T^{\rm UK-RP}_{\rm latency}=&\frac{(1+\rho)(L_{\rm A}+L_{\rm B})+2L_0}{BK}\\ &+\frac{2\left(\frac{(1+\rho)(L_{\rm A}+L_{\rm B})}{\log_2 N_{\rm q}}+L_0\right)}{BK_{\rm s}}+\frac{4d}{c}, \end{aligned} \tag{47}$$

The latency difference between them is

$$\Delta T = T_{\text{latency}}^{\text{UK-RP}} - T_{\text{latency}}^{\text{proposed}} = \frac{2L_0}{BK_{\text{s}}} + \frac{2d}{c} + \frac{(1+\rho)}{BK}\left(\frac{2K(L_{\text{A}}+L_{\text{B}})}{K_{\text{s}}\log_2 N_{\text{q}}} - (L_{\text{A}}+L_{\text{B}}+L_3)\right). \quad (48)$$

In practical implementations, the number of selected uncorrelated subcarriers $K_{\text{s}} = B/W_{\text{c}} = 2BT_{\text{d}}$ is much smaller than K, where W_{c} and T_{d} are the coherence bandwidth and delay spread, respectively. Moreover, N_{q} cannot be too large so that the KDR between Alice and Bob is within the capability of the ECC. As $\mathbf{K}_3$ is used for attack verification, its length L_3 is generally smaller than both L_{A} and L_{B}. Therefore, the last term of (48) should be larger than 0, and $\Delta T > 0$ is obtained. This completes the proof.

APPENDIX C
PROOF OF EQUATION (34)

The error bits in the uplink need be corrected by the ECC (C_1, n_1, k_1, t_1), which should satisfy that $n_1 - k_1 \geq 2t_1 + 1$, so if C_1 achieves the bound of the correction capability, we can obtain that

$$\epsilon_{\text{eq}} = \frac{t_1}{n_1} = \frac{t_1}{L_{\text{B,con}}}. \quad (49)$$

Then, we have

$$L_{\mathbf{syn}''} \geq 2t_1 + 1 = 2\epsilon_{\text{eq}} L_{\text{B,con}} + 1. \quad (50)$$

Similarly, for the downlink error bits corrected by the ECC (C_2, n_2, k_2, t_2), we also derive that

$$L^{(2)}_{\mathbf{syn}''} \geq 2t_2 + 1 = 2\epsilon L_{\text{A,con}} + 1. \quad (51)$$

Note that $\mathbf{K}_3$ is not used to encrypt transmission information, and its leakage in the syndromes will not affect the secure transmission rate. In addition, due to the superposition of SI signal, only α part of $\mathbf{syn}''$ can be perfectly estimated by Eve. Therefore, the length of effective keys for secure transmission can be expressed as

$$L_{\mathbf{K}_{\text{e}}} \leq L_{\text{A}} + L_{\text{B}} - 2\alpha\epsilon_{\text{eq}}(1+\rho)(2L_{\text{B}} + L_{\text{A}}) - 2\epsilon(1+\rho)L_{\text{A}} - 2, \quad (52)$$

where α denotes the proportion of information leakage to Eve, and thus the upper bound of secure transmission rate of the proposed scheme is

$$R_{\text{UB}}^{\text{proposed}} = \frac{\sup\{\text{L}_{\mathbf{K}_{\text{e}}}\}}{T_{\text{latency}}^{\text{proposed}}}, \quad (53)$$

where $\sup\{\cdot\}$ is the supremum. This completes the proof.

REFERENCES

[1] W. Liu, G. Nair, Y. Li, D. Nesic, B. Vucetic, and H. V. Poor, "On the latency, rate, and reliability tradeoff in wireless networked control systems for IIoT," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 723–733, Jan. 2021.

[2] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.

[3] Z. Abdullah, G. Chen, M. A. M. Abdullah, and J. A. Chambers, "Enhanced secrecy performance of multihop IoT networks with cooperative hybrid-duplex jamming," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 161–172, 2021.

[4] A. Fotovvat, G. M. E. Rahman, S. S. Vedaei, and K. A. Wahid, "Comparative performance analysis of lightweight cryptography algorithms for IoT sensor nodes," *IEEE Internet Things J.*, Early access, Dec. 2020.

[5] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.

[6] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138406–138446, 2020.

[7] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 48–54, Oct. 2019.

[8] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, Oct. 2019.

[9] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5176–5186, Aug. 2017.

[10] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, "Secret group-key generation at physical layer for multi-antenna mesh topology," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 18–33, Jan. 2019.

[11] Z. Ji *et al.*, "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 1030–1034, Jan. 2021.

[12] L. Peng, 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 Trans. Mobile Comput.*, vol. 18, no. 3, pp. 507–519, Mar. 2019.

[13] 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 Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12462–12466, Dec. 2018.

[14] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[15] H. Taha and E. Alsusa, "Secret key exchange using private random precoding in MIMO FDD and TDD systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 4823–4833, Jun. 2017.

[16] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1517–1530, Feb. 2016.

[17] Z. Ji *et al.*, "Random shifting intelligent reflecting surface for OTP encrypted data transmission," *IEEE Wireless Commun. Lett.*, Early access, Feb. 2021.

[18] G. Li, A. Hu, J. Zhang, and B. Xiao, "Security analysis of a novel artificial randomness approach for fast key generation," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Singapore, Dec. 2017, pp. 1–6.

[19] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2692–2705, Feb. 2020.

[20] L. Jin, S. Zhang, Y. Lou, X. Xu, and Z. Zhong, "Secret key generation with cross multiplication of two-way random signals," *IEEE Access*, vol. 7, pp. 113065–113080, 2019.

[21] Z. Ma, M. Xiao, Y. Xiao, Z. Pang, H. V. Poor, and B. Vucetic, "High-reliability and low-latency wireless communication for Internet of Things: Challenges, fundamentals, and enabling technologies," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7946–7970, Oct. 2019.

[22] M. Mitev, A. Chorti, and M. Reed, "Optimal resource allocation in joint secret key generation and data transfer schemes," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Tangier, Morocco, 2019, pp. 360–365.

[23] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, Jul. 2018.

[24] L. Jiao, J. Tang, and K. Zeng, "Physical layer key generation using virtual AOA and AOD of mmWave massive MIMO channel," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Beijing, China, May 2018, pp. 1–9.

[25] G. Li, Z. Zhang, J. Zhang, and A. Hu, "Encrypting wireless communications on the fly using one-time pad and key generation," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 357–369, Jan. 2021.

[26] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[27] E. V. Belmega and A. Chorti, "Protecting secret key generation systems against jamming: Energy harvesting and channel hopping approaches," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2611–2626, Nov. 2017.
[28] M. Letafati, A. Kuhestani, K.-K. Wong, and M. J. Piran, "A lightweight secure and resilient transmission scheme for the Internet of Things in the presence of a hostile jammer," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4373–4388, Mar. 2021.
[29] X. Wang, M. Liu, D. Wang, and C. Zhong, "Pilot contamination attack detection using random symbols for massive MIMO systems," in *Proc. Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, Jun. 2017, pp. 1–7.
[30] N. Wang, W. Li, A. Alipour-Fanid, L. Jiao, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for 5G mmWave grant-free IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 658–670, 2021.
[31] S. Chen *et al*., "Learning-based remote channel inference: Feasibility analysis and case study," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3554–3568, Jul. 2019.
[32] Z. Ji *et al*., "Vulnerabilities of physical layer secret key generation against environment reconstruction based attacks," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 693–697, May 2020.
[33] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proc. ACM Special Interest Group on Data Commun. (SIGCOMM)*, New York, NY, USA, Aug. 2013, pp. 375 –386.
[34] B. Debaillie *et al*., "Analog/RF solutions enabling compact full-duplex radios," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1662–1673, Sep. 2014.
[35] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security* vol. 12, no. 5, pp. 1195–1206, May 2017.
[36] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.
[37] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 6–11, Oct. 2019.
[38] REMCOM. (2017). *Wireless InSite 3.2.0 Reference Manual*. [Online]. Available: http://www.remcom.com/wireless-insite
[39] L. Yan, C. Han, and J. Yuan, "A dynamic array-of-subarrays architecture and hybrid precoding algorithms for Terahertz wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 9, pp. 2041–2056, Sep. 2020.
[40] S. Shikhantsov *et al*., "Massive MIMO propagation modeling with user-induced coupling effects using ray-tracing and FDTD," *IEEE J. Sel. Areas Commun.* vol. 38, no. 9, pp. 1955–1963, Sep. 2020.
[41] J. Yang *et al.*, "Ultra-reliable communications for Industrial Internet of Things: Design considerations and channel modeling," *IEEE Netw.*, vol. 33, no. 4, pp. 104–111, Jul./Aug. 2019.

Zijie Ji received the B.S. degree in communication engineering from the Beijing Institute of Technology, Beijing, China, in 2016. He is currently pursuing the Ph.D. degree in information and communication engineering with the School of Information and Electronics, Beijing Institute of Technology, Beijing, China. From 2019 to 2021, he was a visiting student with the School of Electrical and Information Engineering, The University of Sydney, NSW, Australia. His current research interests include physical layer security, secret key generation, artificial intelligent, Internet of Things, and mobile communication.

Phee Lep Yeoh (Member, IEEE) received the B.E. degree (with University Medal) and the Ph.D. degree from the University of Sydney, Australia, in 2004 and 2012, respectively. From 2008 to 2012, he was with the Telecommunications Laboratory at the University of Sydney and the Wireless and Networking Technologies Laboratory at the Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia. From 2012 to 2016, he was with the Department of Electrical and Electronic Engineering at the University of Melbourne, Australia. Since 2016, he has been a Senior Lecturer with the School of Electrical and Information Engineering at the University of Sydney, Australia.

He is a recipient of the 2017 Alexander von Humboldt Research Fellowship for Experienced Researchers and the 2014 Australian Research Council (ARC) Discovery Early Career Researcher Award (DECRA). He has served as TPC chair for the 2016 Australian Communications Theory Workshop (AusCTW) and TPC member for IEEE GLOBECOM, ICC, and VTC conferences. He has received best paper awards at IEEE ICC 2014 and IEEE VTC-Spring 2013, and best student paper awards at AusCTW 2013 and 2019. His current research interests include secure wireless communications, ultra-reliable and low-latency communications (URLLC), ultra-dense networks, and multiscale molecular communications.

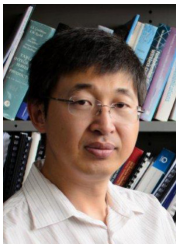
Gaojie Chen (S'09–M'12–SM'18) received the B.Eng. and B.Ec. Degrees in electrical information engineering and international economics and trade from Northwest University, China, in 2006, and the M.Sc. (Hons.) and Ph.D. degrees in electrical and electronic engineering from Loughborough University, Loughborough, U.K., in 2008 and 2012, respectively. After graduation, he took up academic and research positions at DT Mobile, Loughborough University, University of Surrey, University of Oxford and University of Leicester, U.K. He is currently an Assistant Professor with the Institute for Communication Systems, 5GIC & 6GIC, University of Surrey, U.K. His current research interests include information theory, wireless communications, cooperative communications, cognitive radio, the Internet of Things, secrecy communications, and random geometric networks. He received the Exemplary Reviewer Certificates of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2018, the IEEE TRANSACTIONS ON COMMUNICATIONS in 2019 and the IEEE COMMUNICATIONS LETTERS in 2020, and Exemplary Editor of the IEEE COMMUNICATIONS LETTERS in 2021. He serves as an Associate Editor for the IEEE COMMUNICATIONS LETTERS, IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS - MACHINE LEARNING IN COMMUNICATIONS AND NETWORKS and *Electronics Letters* (IET).

Junqing Zhang received the B.Eng and M.Eng degrees in Electrical Engineering from Tianjin University, China in 2009 and 2012, respectively, and the Ph.D degree in Electronics and Electrical Engineering from Queen's University Belfast, UK in 2016. From Feb. 2016 to Jan. 2018, he was a Postdoctoral Research Fellow with Queen's University Belfast. From Feb. 2018 to May 2020, he was a Tenure Track Fellow (Assistant Professor) with University of Liverpool, UK. Since June 2020, he is a Lecturer (Assistant Professor) with University of Liverpool. His research interests include Internet of Things, wireless security, physical layer security, key generation, radio frequency fingerprint identification, and WiFi sensing. He is the receipt of the UK EPSRC New Investigator Award.

Yan Zhang (Member, IEEE) received the B.S. degree in information engineering from the Beijing Institute of Technology, Beijing, China, in 2005, and the Ph.D. degree in information and communication engineering from Tsinghua University, Beijing, China, in 2010. From 2010 to 2013, he was with the Department of Electronic Engineering, Tsinghua University, Beijing, China, as a Post-Doctoral Researcher. From 2014 to 2015, he was a Research Assistant with the School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, U.K. He is currently an Associate Professor with the School of Information and Electronics, Beijing Institute of Technology, Beijing, China. His main research interests include wireless channel modeling, physical layer security, and mobile communication systems.

Zunwen He (Member, IEEE) received the B.S. and M.S. degrees in electromechanical engineering, and Ph.D. degree in information and communication engineering from the Beijing Institute of Technology, Beijing, China, in 1986, 1989, and 2004. He is currently an Associate Professor with the School of Information and Electronics, Beijing Institute of Technology, Beijing, China. His areas of interest are physical layer security, wireless sensor networks, and information systems.

Hao Yin received the B.S. degree in microwave communication and the M.S. degree in communication and information systems from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 1982 and 1987, respectively, and the Ph.D. degree in communication and information systems from the Beijing Institute of Technology, Beijing, China, in 1999. He is currently an Adjunct Professor with the Army Engineering University of PLA, Nanjing, and a Researcher with the Institute of China Electronic System Engineering, Beijing. He is a fellow of the Chinese Academy of Sciences and a fellow of the China Institute of Communications. His research interests include wireless communication networks and information systems.



Yonghui Li (M'04–SM'09–F'19) received his PhD degree in November 2002 from Beijing University of Aeronautics and Astronautics. Since 2003, he has been with the Centre of Excellence in Telecommunications, the University of Sydney, Australia. He is now a Professor and Director of Wireless Engineering Laboratory in School of Electrical and Information Engineering, University of Sydney. He is the recipient of the Australian Queen Elizabeth II Fellowship in 2008 and the Australian Future Fellowship in 2012. He is a Fellow of IEEE.

His current research interests are in the area of wireless communications, with a particular focus on MIMO, millimeter wave communications, machine to machine communications, coding techniques and cooperative communications. He holds a number of patents granted and pending in these fields. He is now an editor for IEEE Transactions on Communications and IEEE Transactions on Vehicular Technology. He was also the guest editor for IEEE JSAC special issue on Millimeter Wave Communications for Future Mobile Networks. He received the best paper awards from IEEE International Conference on Communications (ICC) 2014, IEEE PIMRC 2017 and IEEE Wireless Days Conferences (WD) 2014.