IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 21, 2018, accepted July 5, 2018, date of publication July 25, 2018, date of current version August 20, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2859781

A Collaborative PHY-Aided Technique For End-to-End IoT Device Authentication

PENG HAO[1], (Member, IEEE), XIANBIN WANG[1], (Fellow, IEEE), AND WEIMING SHEN[2], (Fellow, IEEE)

[1]Department of Electrical and Computer Engineering, University of Western Ontario, London, ON N6A 5B9, Canada
[2]National Research Council Canada, Ottawa, ON K1A 0R6, Canada

Corresponding author: Xianbin Wang (xianbin.wang@uwo.ca)

ABSTRACT Nowadays, Internet of Things (IoT) devices are rapidly proliferating to support a vast number of end-to-end (E2E) services and applications, which require reliable device authentication for E2E data security. However, most low-cost IoT end devices with limited computing resources have difficulties in executing the increasingly complicated cryptographic security protocols, resulting in increased vulnerability of the virtual authentication credentials to malicious cryptanalysis. An attacker possessing compromised credentials could be deemed legitimate by the conventional cryptography-based authentication. Although inherently robust to upper-layer unauthorized cryptanalysis, the device-to-device physical-layer (PHY) authentication is practically difficult to be applied to the E2E IoT scenario and to be integrated with the existing, well-established cryptography primitives without any conflict. This paper proposes an enhanced E2E IoT device authentication that achieves seamless integration of PHY security into traditional asymmetric cryptography-based authentication schemes. Exploiting the collaboration of several intermediate nodes (e.g., edge gateway, access point, and full-function device), multiple radio-frequency features of an IoT device can be estimated, quantized, and used in the proposed PHY identity-based cryptography for key protection. A closed-form expression of the generated PHY entropy is derived for measuring the security enhancement. The evaluation results of our cross-layer authentication demonstrate an elevated resistance to various computation-based impersonation attacks. Furthermore, the proposed method does not impose any extra implementation overhead on resource-constrained IoT devices.

INDEX TERMS Device authentication, Internet of Things, physical layer security, collaborative security, radio-frequency fingerprinting, cross-layer security.

I. INTRODUCTION

The Internet of things (IoT) is emerging as the next wave of technological evolution by pervasively supporting wireless devices for diverse end-to-end (E2E) applications and services via the Internet. Densely deployed IoT devices, including low-cost wireless sensors, actuators, and smart objects, are expected to securely and intelligently exchange data with minimal human intervention. Given the importance of E2E data confidentiality and privacy in the areas of industry, healthcare, and financial businesses, robust device authentication is essential before establishing the connectivity of any IoT device [1], [2].

Conventionally, device authentication is implemented at the upper-layer of the security protocol stack using E2E asymmetric encryption [3]–[5], which relies on the hardness of the underlying mathematical problems, namely, computational security [6]. However, critical challenges emerge when using computational security in the context of IoT device authentication.

A. RESEARCH MOTIVATION

From an application perspective, wireless IoT devices are becoming more important and on their way to massive commercial deployment. However, resource-constrained IoT devices could take longer time to execute and update the complicated cryptographic protocols, especially in the scenario of time-consuming E2E credential distribution. Many research efforts have been dedicated to reduce the computational overhead of IoT device authentication. Recently, elliptic curve cryptography (ECC)-based authentication techniques, whose key length can be much shorter than that of RSA, have been studied for IoT [4], [5]. However, shortened

key length implies reduced key space size and lower entropy of the key. According to Shannon's perfect secrecy theory [7], the size of the key space must not be less than the size of the plaintext space to ensure the guessing secrecy [8]. Consequently, resource-limited IoT devices with such shortened keys can be more vulnerable to malicious cryptanalysis. Moreover, sophisticated attackers with rapidly growing processing power are capable of compromising the simplified cryptographic credentials within a much shorter time than before, for example, by using exhaustive search approaches. Since most credentials are virtual numbers (e.g., encryption keys or certificates), any attacker possessing the authorized credentials could be authenticated without triggering any alarms.

Physical-layer-aided authentication is a promising and complementary security paradigm with which to address the above problems due to the inherent physical-layer (PHY) advantages.

- PHY fingerprinting is intrinsically resistant to upper-layer attacks. Different from conventional authentication relying on digital encryption, various PHY characteristics that are directly associated with a wireless communication link and/or a transceiver's radio-frequency (RF) hardware can be exploited for uniquely fingerprinting wireless transmitters.
- The implementation complexity of PHY authentication can be low in device-to-device (D2D) scenarios. At the transmitter (e.g., IoT end devices), all transmitted signals are automatically affected by either environment-dependent wireless channels or transmitter-specific RF front-end imperfections. At the receiver side, both channel and RF imperfection estimations are usually mandatory functions for signal reception. Thus, it is cost-effective to generate a PHY identity (PHY-ID) based on these estimation results. Furthermore, low-cost IoT devices are likely to have more observable RF imperfections for identity differentiation.
- As another source of randomness, PHY can provide additional entropy in order to compensate for the loss of entropy due to using shortened keys in IoT.

Despite many obvious benefits, PHY-aided IoT device authentication is still far from the practical deployment stage due to several technical problems.

1) FROM D2D TO E2E

In practice, the observation of a PHY device fingerprint is mostly restricted to D2D scenarios, whereas in IoT E2E authentication, the real-time PHY features of a source node cannot be directly observed and verified by the destination node, which is located at the other end of the Internet. Hence, the collaboration of intermediate nodes is necessary to extend D2D PHY authentication to E2E scenarios. In practical IoT-enabled networks, the collaborative edge node with enough computing power, such as a gateway, can be exploited to preliminarily process the PHY characteristics and even complete a fast PHY authentication prior to sending the encrypted data from source to destination. In doing so, the E2E delay caused by time-consuming cryptography processing could be avoided.

2) LOW RELIABILITY OF PHY CHARACTERISTICS

Due to the non-stationarity of wireless channels, extensive channel monitoring and frequent adaptation of authentication rules have to be executed within the channel coherence time, which is extremely difficult in a complicated E2E scenario. Furthermore, the coherence time can be significantly decreased in high-frequency communications (e.g., it can be less than 1 ms in mmWave frequency [9]). Although much more stable, the RF characteristic's small value and limited range bring substantial difficulty to the identification of device PHY-ID. In these cases, multi-attributes multi-observations (MAMO) is a promising technique for improving the reliability of the observed PHY characteristics [10].

3) PHY-AIDED CROSS-LAYER SECURITY DESIGN

The cross-layer design requires that 1) the PHY technique be seamlessly integrated into existing, well-established classic cryptography primitives and 2) no additional computational costs be imposed on the resource-limited IoT devices.

4) EFFECTIVE PHY EXPLOITATION

Directly treating (e.g., encrypting/decrypting) PHY characteristics as the shared secret between two authentication terminals is not essentially different from the typical method of using random numbers as the shared secret, especially in the E2E scenario. To fully exploit the inherent resistance of PHY to unauthorized decryption and cryptanalysis, the promising techniques of PHY enhanced public key and identity-based signature need more specific designs [10].

B. RELATED WORK

In [11]–[13], several unclonable PHY features, including carrier frequency offset (CFO), in-phase/quadrature-phase imbalance (IQI), and channel impulse response, are used to identify/authenticate wireless transmitters in D2D scenarios. Physical unclonable function (PUF) is another hardware-dependent PHY authentication technique, which relies on uniquely manufactured integrated circuits (ICs) to generate digital challenge-response pairs (CRPs) and uses these digital CRPs as shared secrets for authentication [14], [15]. Compared to the RF-based methods, PUF must complete many additional processes. The production of ICs can increase manufacturing costs remarkably and additional ICs can be impractical or expensive to retrofit to existing IoT devices [16]. The transmission of CRP signals occupies extra bandwidth, time, and power of the resource-limited IoT devices. These facts impede the seamless integration of PUF with existing infrastructure and authentication protocols.

Regarding PHY-aided cross-layer authentication, Wang *et al.* [10] and Zeng *et al.* [16] proposed some constructive ideas such as MAMO and a composite security

key. In [17] and [18], cooperative IoT devices are adopted for enhancing E2E communication security. Given the dense deployment of IoT devices, collaborative node-based MAMO has significant potential to resolve the problem of *low reliability of PHY characteristics*. However, applying these ideas to practical IoT E2E authentication still brings with it several of the above-mentioned technical problems yet to be addressed. In [19], several PHY parameters were employed as the shared secret for cross-layer authentication. This method simply considers ideally estimated PHY features and, again, has no difference from using random virtual numbers in E2E scenario. In [20] and [21], lightweight identity-based cryptography (IBC) techniques are proposed to avoid time-consuming certificate mechanisms, which are suitable for constrained IoT devices. Contrary to the PHY-ID, their identities are programmable strings, and thus cannot prevent malicious upper-layer cryptanalysis.

C. CONTRIBUTIONS AND PAPER ORGANIZATION

This paper proposes a PHY-aided enhancement technique for E2E IoT device authentication. We consider an E2E communication system that consists of a source node (e.g., an IoT end device), some collaborative nodes (e.g., edge gateway, access point, and full-function device), and a destination node at the other communication end. With the aid of collaborative nodes, the source-node-associated RF features, including CFO and IQI, can be estimated, dynamically quantized, and used to generate a unique PHY-ID. This PHY-ID is further applied in our cross-layer authentication and the proposed PHY-IBC-based key protection.

The main contributions of this paper are summarized as follows:

- By exploiting collaborative nodes, we achieve seamless integration of D2D PHY fingerprinting with the conventional asymmetric cryptography-based E2E IoT device authentication. In doing so, our method achieves certificate-free PHY-IBC and attains improved resistance to most upper-layer computation-based impersonation attacks.
- Rather than assuming the perfect RF feature estimates, the practically estimated PHY parameters are considered in generating the PHY-IDs of IoT devices.
- Using MAMO, we achieve increased detection probability and accomplish PHY-IBC-based key protection with the proposed PHY-ID. Furthermore, we derive a closed-form expression for the PHY entropy as the measure of our security enhancement.
- The proposed PHY-aided authentication scheme does not impose any additional computational overhead on the resource-constrained IoT devices. Using our two-step authentication design, we can even reduce the authentication time in the case of dealing with a small group of devices in the presence of attackers.

The remainder of this paper is organized as follows. Section II presents the preliminaries, including the IBC technique, PHY characteristic selection, and notations. In Section III, the framework of the proposed PHY-aided authentication system is described. Section IV presents the technique for practically estimating CFO, IQI, and wireless channels. The proposed registration phase and authentication phase are described in Section V and VI, respectively. Section VII evaluates the authentication performance and security strength when opposed by different adversaries. Finally, Section VIII presents the conclusions and discuss the future work.

II. PRELIMINARIES

A. IDENTITY-BASED CRYPTOGRAPHY

In IBC, the public key of an entity can be either a string that corresponds to this entity's identity information or straightforwardly computed from the identity. A typical example of the identity in IBC is a user's email address, which is unique and publicly verifiable. Since there is no need to validate the meaningful identity-associated public key, the certificate mechanism, including certificate storage, distribution and revocation, is no longer needed. Therefore, IBC is certificate-free, which makes it suitable for the resource-limited IoT [22].

To make IoT device authentication certificate-free, we need to find appropriate PHY-IDs of IoT devices. According to the working principle of IBC, an eligible PHY-ID must meet the following requirements:

- *Uniquely Associated:* Like the email address of a person, the eligible PHY-ID should be uniquely associated with an IoT device for authentication.
- *Publicly Verifiable and Reliable:* In IBC, the email address of a user can be publicly known, verifiable, and always be fixed. Similarly, the eligible PHY-ID of a device must be publicly accessible and verifiable. Also, this PHY-ID should be reliable, for example, it cannot be fast varying and easily programmable.

B. PHY CHARACTERISTIC SELECTION

In general PHY authentication, PHY characteristics can be classified as channel-based characteristics and RF-based characteristics. The selected PHY characteristics should be applicable under the conditions of E2E IoT security.

Since the wireless channel features of a transmitter-receiver pair can be significantly different from those of other transmitter-receiver pairs, characteristics such as channel state information [23] and received signal strength indicator [24] can be continuously monitored at the receiver to determine whether or not the current transmitter is the same as the last authorized transmitter. This type of technique always requires extensive channel monitoring and frequent adaptation of the authentication rules, as a channel can significantly change beyond the channel coherence time. Furthermore, the coherence time is inversely proportional to the maximum Doppler frequency. In the future, channel coherence time can be remarkably shortened in high-frequency communications, e.g., much less than 1 ms at mmWave frequency of 5G [9]. Such frequent channel monitoring

TABLE 1. Notations.

Notations	Descriptions
SN, SN-A/B	Source node, source node A/B
LSN, ISN	Legitimate SN, Illegitimate SN
CN_i, SCN_i	Collaborative node, selected CN_i
DN	Destination node
AP	Access point
KGC	Key generation center
$PubK_A$	Public key of SN-A
$PvtK_A$	Private key of SN-A
PHY-ID	PHY identity of an IoT end device
$CFO\text{-}ID$	CFO-based identity
$IQI\text{-}ID$	IQI-based identity
PHY-IBC	PHY identity-based cryptography
$h(\cdot)$	One-way hash function
$f(\cdot)$	User-defined function

and updating are challenging even in D2D authentication, let alone in the complicated E2E scenario.

RF imperfections of a device are introduced during the fabrication of the RF-chain's analog components, and can differ from device to device due to fabrication variations. All signals that are ejected through the imperfect RF front-end are inevitably affected by the device-specific RF features. Given that it is practically impossible to arbitrarily change hardware-level RF features in a short time [10], [11], [16], [25], [26], RF-based IQI [12] and CFO [11] can be observed by receiver to accurately fingerprint the transmitters. In addition, CFO and IQI are sufficiently stable to remain steady over the time scale of hours and days [27], which is usually much longer than an E2E authentication session. CFO and IQI can meet all above-mentioned requirements of IBC since they are reliable, uniquely associated with the RF hardware of an IoT device, and publicly observable and verifiable by the signal receivers. However, the value of hardware imperfection is usually small and range-limited, thereby resulting in difficulty in distinguishing the minor differences of CFO and IQI between different devices. As reported in [10], the MAMO technique can resolve this limited-range problem.

Consequently, RF-based characteristics are more suitable than channel-based characteristics for IoT E2E device authentication.

C. LIST OF NOTATIONS

$(\cdot)^*$, $|\cdot|$, $(\cdot)^T$, $(\cdot)^H$, and $||$ denote conjugate, absolute value, transpose, conjugate transpose, and bitwise concatenation operations, respectively. Bold lowercase and uppercase letters represent vectors and matrices. $\Re(x)$ and $\Im(x)$ denote the real part and imaginary part of x. In addition, Table 1 shows the rest notations.

III. SYSTEM FRAMEWORK DESCRIPTION

We consider a typical E2E communication system in the context of IoT, where the two ends are a source node (SN), e.g., an IoT end device, and a destination node (DN), e.g., an Internet host. However, the illegitimate SN (ISN) may be present in a group of legitimate SNs (LSNs) by impersonating an LSN during any available communication time slot, which gives rise to the demand of authenticating SN at the DN side. Since SN must send messages to DN via some intermediate nodes in the E2E scenario, we consider the intermediate nodes that share the direct link with SN as collaborative nodes (CNs). Eligible CNs are located within the communication coverage of SN and can simultaneously receive the signals of SN in a time instant. We assume that the network association, authentication and synchronization of CNs have already been completed before receiving signals of SN. In practice, CN can be an access point, an edge gateway, and/or a full-function device in IoT-enabled networks. Given the trend of dense deployment of IoT networks, more CNs will be available in future E2E communications [17].

Without loss of generality, it is assumed that SN is working in sense-and-send mode and using asymmetric cryptography for authentication. In a conventional asymmetric cryptography method, SN encrypts the sensed data using its *PvtK* to generate the unique signature, and sends the encrypted message to DN. DN, with the correct *PubK* of SN, is able to verify the signature and obtain the readable plaintext, and thus authenticate SN. As mentioned earlier, resource-limited IoT devices with shorter *PvtK* are more vulnerable to the malicious cryptanalysis. Moreover, given the hardness of figuring out *PvtK*, sophisticated attackers can alternatively spoof the *PubK*. For example, if DN uses the *PubK* of an ISN, the authentication system can be cracked since the received message signature can be generated by ISN's *PvtK*. Therefore, Diffie-Hellman exchange-based certificate management is usually required to safeguard the *PubK*.

Our objective is to exploit the RF features of SN to enhance the conventional authentication in terms of boosting the system resistance to upper-layer computation-based attacks, providing additional PHY entropy to protect keys, and avoiding the time-consuming certificate mechanism through using PHY-IBC. In addition, the authentication enhancement should not impose any extra computational overhead on the resource-limited SN.

Fig. 1 shows the considered E2E authentication architecture, where SN-A sends the sensed data to DN via the main link. Our PHY-aided authentication enhancement can be integrated into the registration and authentication phases, which are mandatory in most asymmetric cryptography-based authentication schemes. The block diagrams in Fig. 2 and 3 show the main processes of these two phases.

The registration phase aims to register the credentials of SN-A, including the PHY CFO/IQI and the upper-layer encryption keys. In this phase, SN-A selects N CNs from M available CNs for collaboration, where $M \geqslant N \geqslant 1$. The selected CNs are represented by SCN_i, where $i = 1, 2, \cdots, N$. In the example of Fig. 1, $M = 5$, $N = 3$, and the selected CNs are SCN_1, SCN_2 and SCN_3. Only the SCN_1 in the main link is necessary in our authentication,

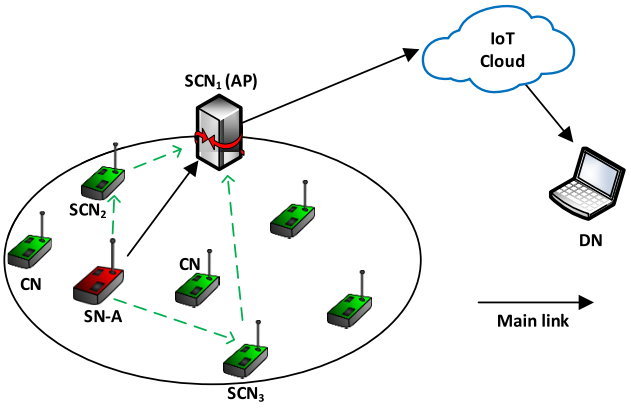


FIGURE 1. Collaborative E2E IoT device authentication architecture.

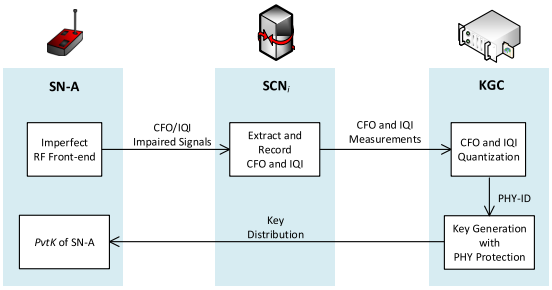


FIGURE 2. Main procedures of registration phase.

while all other SCN$_i$, $i \neq 1$, are optional. SCN$_i$, $i \neq 1$ only collaborates for authentication, not for the delivery of the sensed data. Since CFO and IQI automatically affect all signals transmitted by SN-A, any message (e.g., association request, hello message, handshake message or sensed data) that is directly received by an SCN$_i$ can be analyzed to extract the CFO and IQI parameters of SN-A. Therefore, our PHY-aided method can be used in existing cryptography schemes without requiring extra signal transmission. Then, SCNs can forward the estimated parameters to a key generation center (KGC), who is responsible for the encryption key generation and distribution, as commonly utilized in public-key cryptosystems [28]. Given that our method does not revise the existing key management, the upper-layer key generation and distribution are outside the scope of this paper. These CFO/IQI parameters can be quantized to bits with different quantization rules, and are thereafter used to generate a unique PHY-ID of SN-A. This PHY-ID is further applied in the authentication phase and a proposed PHY-IBC-based key protection scheme. In addition, the above-mentioned MAMO technique is realized 1) by using two RF features, including CFO and IQI, and 2) by different CFO and IQI observations from multiple SCNs.

The authentication phase can be executed to determine whether the current SN is the registered SN-A or an ISN. With the aid of SCNs, the CFO and IQI-based PHY-ID of the SN and the PHY-enhanced key are utilized in our two-step authentication process, as shown in Fig. 3.

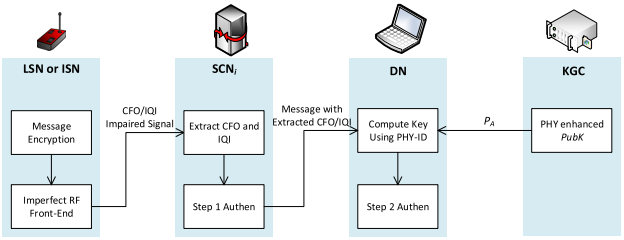


FIGURE 3. Main procedures of authentication phase.

In the remainder of the paper, we follow the processing flow to describe the detailed CFO/IQI estimation technique, the PHY-enhanced registration process and the two-step authentication procedure.

IV. PHY CFO, IQI AND CHANNEL ESTIMATION AT SCN$_i$

In this section, we first present the signal model in the presence of CFO and IQI between SN and SCN$_i$. Then, we propose a CFO, IQI and channel estimation method. For simplicity of presentation, our analysis focuses on a single SCN$_i$; the same processes can be executed at other SCNs. Subscript A in x_{A} and subscript i in x_i denote SN-A and SCN$_i$, respectively. We use $x_{\mathrm{A},i}$ to denote the variable between SN-A and SCN$_i$ in the following.

A. SIGNAL MODELING WITH CFO AND IQI

CFO is caused by the inevitable synchronization error between two oscillators that are installed in transmitter (i.e., SN-A) and receiver (i.e., SCN$_i$). IQI mainly refers to amplitude and phase mismatches between in-phase (I) and quadrature-phase (Q) branches in a transceiver's I/Q signal processing [29]. Hence, CFO and IQI are considered as independent RF characteristics. Also, it is assumed that the stable hardware-level CFO and IQI are constant during the E2E authentication procedure [11], [27], [30], [31]. We consider an OFDM system in which all wireless entities are operating with single antenna. At the SN-A side, after taking the inverse discrete Fourier transform, the $K \times 1$ symbol vector in a time instant is denoted as $\mathbf{d} = [d_0\ d_1 \cdots d_{K-1}]^T$ with average power $P = \mathbb{E}[d_k^* d_k]$, $k = 0, 1, 2, \cdots, K-1$. We use the asymmetric IQI model [32], [33], in which the signal is affected by Tx/Rx gain imbalance $\alpha_{\mathrm{tx/rx}}$ and phase-shift imbalance $\theta_{\mathrm{tx/rx}}$. Thus, the signal distorted by SN-A's Tx IQI is expressed by [33][1]

$$\mathbf{s} = \mu_{\mathrm{A}}\mathbf{d} + \nu_{\mathrm{A}}\mathbf{d}^* \tag{1}$$

where μ_{A} and ν_{A} are the unique IQI parameters of SN-A as

$$\mu_{\mathrm{A}} = \frac{1}{2}[1 + (1+\alpha_{\mathrm{tx}})e^{j\theta_{\mathrm{tx}}}], \tag{2}$$

$$\nu_{\mathrm{A}} = \frac{1}{2}[1 - (1+\alpha_{\mathrm{tx}})e^{j\theta_{\mathrm{tx}}}] = 1 - \mu_{\mathrm{A}}. \tag{3}$$

[1]Note that $1+\alpha_{\mathrm{tx}}$ in our paper is equivalent to the amplitude mismatch used in [33].

After experiencing a multi-path channel, the received signal at SCN_i without CFO and IQI of SCN_i is

$$\mathbf{y}_i = \mathbf{H}_i\mathbf{s} + \mathbf{w}_i \tag{4}$$

where $\mathbf{H}_i$ denotes the $K \times K$ circulant channel matrix with the first column formed by an $L \times 1$ channel impulse response vector $\mathbf{h}_i = [h_0\ h_1 \cdots h_{L-1}]^T$. The representation of $\mathbf{H}_i$ is

$$\mathbf{H}_i = \begin{bmatrix} h_0 & 0 & \cdots & h_2 & h_1 \\ h_1 & h_0 & \cdots & & \vdots \\ \vdots & \vdots & \ddots & \ddots & h_{L-1} \\ h_{L-1} & h_{L-2} & & & 0 \\ 0 & h_{L-1} & \ddots & \ddots & \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & h_1 & h_0 \end{bmatrix} \tag{5}$$

and the elements of noise term $\mathbf{w}_i$ are independent and identically distributed (i.i.d.) complex circularly symmetric Gaussian variables. Defining $\varepsilon_{\text{A},i}$ as the normalized CFO between SN-A and SCN_i, we can get a $K \times K$ diagonal matrix [34]

$$\mathbf{C}_i \triangleq diag[1\ \ e^{j\frac{2\pi\varepsilon_{\text{A},i}}{K}}\ \ e^{j\frac{4\pi\varepsilon_{\text{A},i}}{K}}\ \ \cdots\ e^{j\frac{2\pi(K-1)\varepsilon_{\text{A},i}}{K}}]. \tag{6}$$

The baseband equivalent signal with the presence of CFO and Rx IQI of SCN_i is given by

$$\begin{aligned}\mathbf{z}_i &= \mu_i\mathbf{C}_i\mathbf{y}_i + \nu_i(\mathbf{C}_i\mathbf{y}_i)^* \\ &= (k_1\mathbf{C}_h + k_2\mathbf{C}_h^*)\mathbf{d} + (k_3\mathbf{C}_h + k_4\mathbf{C}_h^*)\mathbf{d}^* + \mathbf{w}_{z_i}\end{aligned} \tag{7}$$

where $\mathbf{C}_h = \mathbf{C}_i\mathbf{H}_i$, $\mathbf{w}_{z_i}$ is the noise term, and the receiving IQI parameters of SCN_i are

$$\mu_i = \frac{1}{2}[1 + (1+\alpha_{\text{rx}})e^{-j\theta_{\text{rx}}}], \tag{8}$$

$$\nu_i = \frac{1}{2}[1 - (1+\alpha_{\text{rx}})e^{j\theta_{\text{rx}}}] = 1 - \mu_i^* \tag{9}$$

and

$$k_1 = \mu_i\mu_{\text{A}}, \quad k_2 = \nu_i\nu_{\text{A}}^*,\ k_3 = \mu_i\nu_{\text{A}},\ k_4 = \nu_i\mu_{\text{A}}^*. \tag{10}$$

B. CFO ESTIMATION

We consider the repeated training sequence, whose structure is described in [35] and [36]. Using (7), the two repeated signals can be represented as

$$\mathbf{z}_1' = \mu_i\mathbf{r} + \nu_i\mathbf{r}^* + \mathbf{w}_{z_1}' \tag{11a}$$

$$\mathbf{z}_2' = \mu_i\mathbf{r}e^{j2\pi\varepsilon_{\text{A},i}} + \nu_i\mathbf{r}^*e^{-j2\pi\varepsilon_{\text{A},i}} + \mathbf{w}_{z_2}' \tag{11b}$$

where $\mathbf{r} = \mathbf{C}_i\mathbf{y}_i$ denotes the signal in the absence of noise, and the corresponding noise terms are $\mathbf{w}_{z_1}'$ and $\mathbf{w}_{z_2}'$. Assuming that SCN_i has the knowledge of its own IQI information (i.e., μ_i and ν_i), the CFO can be estimated as [36, eq. (52)]

$$\hat{\varepsilon}_{\text{A},i} = \frac{1}{2\pi}\tan^{-1}\left(\frac{\Im((\mathbf{z}_1' - a_i\mathbf{z}_1'^*)^H(\mathbf{z}_2' - a_i\mathbf{z}_2'^*))}{\Re((\mathbf{z}_1' - a_i\mathbf{z}_1'^*)^H(\mathbf{z}_2' - a_i\mathbf{z}_2'^*))}\right) \tag{12}$$

where a_i is defined as $a_i \triangleq \frac{\nu_i}{\mu_i^*}$.

C. IQI AND CHANNEL ESTIMATION

This subsection estimates IQI and channel in the presence of CFO. We rewrite $\mathbf{z}_i$ in (7) as

$$\begin{aligned}\mathbf{z}_i &= \mathbf{C}_i(k_1\mathbf{D} + k_3\mathbf{D}^*)\mathbf{h}_i + \mathbf{C}_i^*(k_2\mathbf{D} + k_4\mathbf{D}^*)\mathbf{h}_i^* + \mathbf{w}_{z_i} \\ &= \mathbf{A}_i\mathbf{b}_i + \mathbf{w}_{z_i}\end{aligned} \tag{13}$$

where $\mathbf{D}$ is the $K \times L$ circulant matrix satisfying $\mathbf{D}\mathbf{h}_i = \mathbf{H}_i\mathbf{d}$, and can be expressed by

$$\mathbf{D} = \begin{bmatrix} d_0 & d_{K-1} & \cdots & d_{K-L+1} \\ d_1 & d_0 & \cdots & d_{K-L+2} \\ \vdots & \vdots & \ddots & \vdots \\ d_{K-1} & d_{K-2} & \cdots & d_{K-L} \end{bmatrix}, \tag{14}$$

$\mathbf{C}_i$ can be calculated by substituting $\hat{\varepsilon}_{\text{A},i}$ obtained from (12) into (6), and $\mathbf{A}_i$ and $\mathbf{b}_i$ can be given by

$$\mathbf{A}_i = \begin{bmatrix}\mathbf{C}_i\mathbf{D} & \mathbf{C}_i^*\mathbf{D} & \mathbf{C}_i\mathbf{D}^* & \mathbf{C}_i^*\mathbf{D}^*\end{bmatrix}_{K\times 4L} \tag{15}$$

$$\mathbf{b}_i = \begin{bmatrix}k_1\mathbf{h}_i^T & k_2\mathbf{h}_i^H & k_3\mathbf{h}_i^T & k_4\mathbf{h}_i^H\end{bmatrix}^T. \tag{16}$$

Using least square (LS) estimation, $\mathbf{b}_i$ can be estimated by

$$\hat{\mathbf{b}}_i = (\mathbf{A}_i^H\mathbf{A}_i)^{-1}\mathbf{A}_i^H\mathbf{z}_i = \begin{bmatrix}\hat{\mathbf{b}}_{g1} & \hat{\mathbf{b}}_{g2} & \hat{\mathbf{b}}_{g3} & \hat{\mathbf{b}}_{g4}\end{bmatrix}^T \tag{17}$$

where $\hat{\mathbf{b}}_{g1}$, $\hat{\mathbf{b}}_{g2}$, $\hat{\mathbf{b}}_{g3}$ and $\hat{\mathbf{b}}_{g4}$ correspond to the estimated version of $k_1\mathbf{h}_i^T$, $k_2\mathbf{h}_i^H$, $k_3\mathbf{h}_i^T$ and $k_4\mathbf{h}_i^H$ in (16), respectively.

Defining

$$\mathbf{g}_1 = \hat{\mathbf{b}}_{g1} + \hat{\mathbf{b}}_{g2}, \quad \mathbf{g}_2 = \hat{\mathbf{b}}_{g3} + \hat{\mathbf{b}}_{g4}, \tag{18}$$

$$\mathbf{H}_b = \begin{bmatrix}\mathbf{h}_i & \mathbf{h}_i^* & 0 & 0 \\ 0 & 0 & \mathbf{h}_i & \mathbf{h}_i^*\end{bmatrix}, \tag{19}$$

$$\mathbf{k} = [k_1\ \ k_2\ \ k_3\ \ k_4]^T, \tag{20}$$

we can obtain an estimation vector as

$$\hat{\mathbf{g}} = [\mathbf{g}_1^T\ \ \mathbf{g}_2^T]^T = \mathbf{H}_b\mathbf{k} + \mathbf{w}_g \tag{21}$$

Therefore, the LS estimation of $\mathbf{k}$ is

$$\hat{\mathbf{k}} = (\mathbf{H}_b^H\mathbf{H}_b)^{-1}\mathbf{H}_b^H\hat{\mathbf{g}}. \tag{22}$$

Then, we can set

$$\begin{aligned}\hat{\mathbf{G}}_0 &= [\Re(\mathbf{g}_1)\ \ \Im(\mathbf{g}_1)\ \ \Re(\mathbf{g}_2)\ \ \Im(\mathbf{g}_2)]^T \\ &= \mathbf{K}_0\mathbf{H}_0 + \mathbf{W}_0\end{aligned} \tag{23}$$

and

$$\mathbf{H}_0 = [\Re(\mathbf{h}_i)\ \ \Im(\mathbf{h}_i)]^T, \tag{24}$$

$$\mathbf{K}_0 = \begin{bmatrix}\Re(k_1) + \Re(k_2) & \Im(k_2) - \Im(k_1) \\ \Im(k_1) + \Im(k_2) & \Re(k_1) - \Re(k_2) \\ \Re(k_3) + \Re(k_4) & \Im(k_4) - \Im(k_3) \\ \Im(k_3) + \Im(k_4) & \Re(k_3) - \Re(k_4)\end{bmatrix} \tag{25}$$

and get the LS estimation of $\mathbf{H}_0$ as

$$\hat{\mathbf{H}}_0 = (\mathbf{K}_0^T\mathbf{K}_0)^{-1}\mathbf{K}_0^T\hat{\mathbf{G}}_0 \tag{26}$$

Based on the above derivations, the IQI and channel estimation procedure is summarized in Algorithm 1. In practice, k_1 is close to 1, while k_2, k_3, and $k_4 \approx 0$. Therefore,

Algorithm 1 IQI and Channel Estimation

1: Initialization:
Calculate $\mathbf{A}_i$ using (15) and $\mathbf{D}$ using (14).
Estimate $\hat{\mathbf{b}}_i$ using (17), and formulate $\hat{\mathbf{g}}$ using (18) (21).
Set $\mathbf{h}_i = \hat{\mathbf{b}}_{g1}$, assign a positive integer to j_{max} as the maximal iteration number, and set $j = 0$.
2: Obtain $\mathbf{H}_b$ by substituting $\mathbf{h}_i$ in (19).
3: Perform the estimation in (22) with $\mathbf{H}_b$ and $\hat{\mathbf{g}}$ to get $\hat{\mathbf{k}}$.
4: Obtain $\hat{\mathbf{G}}_0$ by substituting $\hat{\mathbf{g}}$ in (23).
5: Construct $\mathbf{K}_0$ by substituting $\hat{\mathbf{k}}$ in (25).
6: Calculate $\hat{\mathbf{H}}_0$ using (26).
7: Set $j = j + 1$, and update $\hat{\mathbf{g}}$ and $\mathbf{h}_i$ with $\hat{\mathbf{k}}$ estimated in Step 3 and $\hat{\mathbf{H}}_0$ estimated in Step 6. If $j < j_{max}$, go to Step 2; otherwise, go to Step 8.
8: End of the algorithm.

it is common to set the initial value as $k_1 = 1$ [36]–[39], which results in $\mathbf{h}_i = \hat{\mathbf{b}}_{g1}$ in the initialization step. In our method, the distinguishability of $\hat{k}_1$ is weaker than those of $\hat{k}_2, \hat{k}_3$, and $\hat{k}_4$ due to the initialization setup with $k_1 = 1$. After performing Algorithm 1, we can estimate $\hat{\mathbf{k}}$, obtain $\hat{\mu}_{\mathrm{A},i} = \left(\frac{\hat{k}_4}{\nu_i}\right)^*$, and determine channel $\mathbf{h}_i$. In the following, we use the practically estimated CFO and IQI in the PHY-enhanced registration and authentication phases.

V. PHY-ENHANCED REGISTRATION PHASE

This section presents the PHY-enhanced registration phase (shown in Fig. 2). Based on the estimation technique in the previous section, all N SCNs can send the estimated $(\hat{\varepsilon}_{\mathrm{A},i}, \hat{\mu}_{\mathrm{A},i})$ to KGC via AP. Then, each $(\hat{\varepsilon}_{\mathrm{A},i}, \hat{\mu}_{\mathrm{A},i})$ is quantized at AP and used in the PHY key protection scheme at KGC.

A. CFO AND IQI QUANTIZATION

1) QUANTIZER DESIGN FOR CFO

We suppose that $\varepsilon_{\mathrm{A},i}$ is uniformly distributed as $\varepsilon_{\mathrm{A},i} \sim U(-\varepsilon_m, \varepsilon_m)$, $\varepsilon_m > 0$ [11] with zero mean and variance $\sigma_\varepsilon^2 = \frac{\varepsilon_m^2}{3}$. Its probability density function (PDF) is

$$f_\varepsilon(x) = \frac{1}{2\varepsilon_m}, x \in [-\varepsilon_m, \varepsilon_m] \tag{27}$$

Given fixed K_i quantization levels, the step size of the uniform quantizer is

$$\Delta_{\mathrm{CFO},i} = \frac{2\varepsilon_m}{K_i}, \tag{28}$$

In this case, the decision boundarie of an interval is

$$b_{I,i} = -\varepsilon_m + \Delta_{\mathrm{CFO},i} I \tag{29}$$

where $I = 0, 1, 2, \cdots, K_i$ denotes the quantization index. The quantized CFO value of a decision interval is defined as

$$\begin{aligned} Q(\hat{\varepsilon}_{\mathrm{A},i}) &= \varepsilon_{[k,i]} \\ &= -\varepsilon_m + \Delta_{\mathrm{CFO},i}(k - 0.5), \quad k = 1, 2, \cdots, K_i \end{aligned} \tag{30}$$

Given the quantization rule, the probability mass function (PMF) of the quantized $\varepsilon_{[k,i]}$ can be derived as

$$\tilde{f}_\varepsilon(\varepsilon_{[k,i]}) = \int_{\frac{\varepsilon_m(2k-K_i)}{K_i}}^{\frac{\varepsilon_m(2k+2-K_i)}{K_i}} f_\varepsilon(x)dx = \frac{\Delta_{\mathrm{CFO},i}}{2\varepsilon_m} \tag{31}$$

2) QUANTIZER DESIGN FOR IQI

We consider $\theta_{\mathrm{tx}} \sim U(-\theta_m, \theta_m)$, $\alpha_{\mathrm{tx}} \sim U(-\alpha_m, \alpha_m)$ [40], where $\theta_m > 0$, $\alpha_m > 0$; thus their PDFs are

$$f_\alpha(x) = \frac{1}{2\alpha_m}, \quad x \in [-\alpha_m, \alpha_m] \tag{32}$$

$$f_\theta(x) = \frac{1}{2\theta_m}, \quad x \in [-\theta_m, \theta_m] \tag{33}$$

From (2) (3), $\Re(\mu_{\mathrm{A}}) = 1/2 + 1/2(1 + \alpha_{\mathrm{tx}})\cos\theta_{\mathrm{tx}}$ and $\Im(\mu_{\mathrm{A}}) = 1/2(1 + \alpha_{\mathrm{tx}})\sin\theta_{\mathrm{tx}}$. Hence, the PDF of $\Re(\mu_{\mathrm{A}})$ equals the PDF of $\Re(\nu_{\mathrm{A}})$ multiplied by 2. We consider $r_{\mathrm{A},i} = \Re(\mu_{\mathrm{A}}) - 0.5$ in the IQI quantizer design. Since $\alpha_{\mathrm{tx}} \in [-\alpha_m, \alpha_m]$ and $\theta_{\mathrm{tx}} \in [-\theta_m, \theta_m]$, we have $r_{\mathrm{A},i} \in [0.5(1-\alpha_m)\cos\theta_m, 0.5(1+\alpha_m)]$. Given P_i quantization levels, the step size, decision boundaries, and quantized values of IQI are

$$\Delta_{\mathrm{IQI},i} = \frac{\alpha_m(1 + \cos\theta_m) + 1 - \cos\theta_m}{2P_i} \tag{34}$$

$$b_{J,i} = \frac{(1-\alpha_m)\cos\theta_m + 2\Delta_{\mathrm{IQI},i}J}{2}, \quad J = 0, 1 \cdots, P_i \tag{35}$$

$$\begin{aligned} Q(\hat{r}_{\mathrm{A},i}) &= r_{[p,i]} \\ &= \frac{(1-\alpha_m)\cos\theta_m + \Delta_{\mathrm{IQI},i}(2p-1)}{2}, \quad p = 1, \cdots, P_i \end{aligned} \tag{36}$$

where $\hat{r}_{\mathrm{A},i} = \Re(\hat{\mu}_{\mathrm{A},i}) - 0.5$.

We define $A = \frac{1}{\theta_m\alpha_m}$, $B = \frac{(1-\alpha_m)\cos\theta_m}{2}$, $C = \frac{(1+\alpha_m)\cos\theta_m}{2}$, $D = \frac{1}{\cos\theta_m}$, and derive the PDF of $r_{\mathrm{A},i}$ in three cases as follows.

If $\alpha_m < -\frac{\cos\theta_m - 1}{\cos\theta_m + 1}$,

$$f_r(x) = \begin{cases} A\ln\left(\dfrac{xD + \sqrt{(xD)^2 - x^2}}{BD + \sqrt{(BD)^2 - x^2}}\right), & x \in [B, C) \\ A\ln\left(\dfrac{CD + \sqrt{(CD)^2 - x^2}}{BD + \sqrt{(BD)^2 - x^2}}\right), & x \in [C, BD) \\ A\ln\left(\dfrac{CD}{x} + \sqrt{\left(\frac{CD}{x}\right)^2 - 1}\right), & x \in [BD, CD] \end{cases} \tag{37}$$

If $\alpha_m > -\frac{\cos\theta_m - 1}{\cos\theta_m + 1}$,

$$f_r(x) = \begin{cases} A\ln\left(\dfrac{xD + \sqrt{(xD)^2 - x^2}}{BD + \sqrt{(BD)^2 - x^2}}\right), & x \in [B, BD) \\ A\ln\left(D + \sqrt{D^2 - 1}\right), & x \in [BD, C) \\ A\ln\left(\dfrac{CD}{x} + \sqrt{\left(\dfrac{CD}{x}\right)^2 - 1}\right), & x \in [C, CD] \end{cases} \tag{38}$$

If $\alpha_m = -\frac{\cos\theta_m - 1}{\cos\theta_m + 1}$,

$$f_r(x) = \begin{cases} A\ln\left(\dfrac{xD + \sqrt{(xD)^2 - x^2}}{BD + \sqrt{(BD)^2 - x^2}}\right), & x \in [B, BD) \\ A\ln\left(\dfrac{CD}{x} + \sqrt{\left(\frac{CD}{x}\right)^2 - 1}\right), & x \in [BD, CD] \end{cases} \tag{39}$$

Based on (37), (38) and (39), the PMF of the discrete quantized values can be derived as

$$\tilde{f}_r(r_{[p,i]}) = \int_{B+p\Delta_{\mathrm{IQI},i}}^{B+(p+1)\Delta_{\mathrm{IQI},i}} f_r(x)dx \tag{40}$$

Through quantizing CFO and IQI parameters, AP can obtain $K_i \times P_i$ possible random variables $Q_i = (\varepsilon_{[k,i]}, r_{[p,i]})$. The PHY domain Q_i can be integrated into the asymmetric key scheme to elevate the encryption key's resistance to upper-layer attacks as well as provide additional entropy to the key for improving the guessing secrecy. Since CFO and IQI are independent characteristics, the entropy of Q_i can be derived based on (31) and (40), as given by

$$H_i = H_{\mathrm{CFO},i} + H_{\mathrm{IQI},i} \tag{41}$$

where

$$H_{\mathrm{CFO},i} = -\sum_{k=1}^{K_i} \tilde{f}_\varepsilon(\varepsilon_{[k,i]}) \log_2(\tilde{f}_\varepsilon(\varepsilon_{[k,i]})) \tag{42}$$

$$H_{\mathrm{IQI},i} = -\sum_{p=1}^{P_i} \tilde{f}_r(r_{[p,i]}) \log_2(\tilde{f}_r(r_{[p,i]})) \tag{43}$$

where $H_{\mathrm{CFO},i}$ denotes the CFO entropy generated by SCN_i, and $H_{\mathrm{IQI},i}$ denotes the IQI entropy generated by SCN_i.

B. PHY-IBC KEY PROTECTION

Given the public sharing nature of $PubK$ and the hardness of figuring out $PvtK$, $PubK$ is usually more vulnerable than $PvtK$ in practice. For example, if DN uses the $PubK$ of an ISN, DN will be spoofed since the received signature can be generated by the ISN's $PvtK$. Motivated by the advantages of IBC, we propose a PHY-ID that is composed of Q_i for protecting the true $PubK_A$ of SN-A.

In the registration phase, KGC generates the key pair ($PvtK_A$ and $PubK_A$) and securely sends $PvtK_A$ to SN-A, as required by the asymmetric cryptography-based schemes. After receiving Q_i from AP, KGC further computes

$$CFO\text{-}ID_{\mathrm{A}} = Q(\hat{\varepsilon}_{\mathrm{A},1})||Q(\hat{\varepsilon}_{\mathrm{A},2})||\cdots||Q(\hat{\varepsilon}_{\mathrm{A},N}) \tag{44}$$

$$IQI\text{-}ID_{\mathrm{A}} = Q(\hat{r}_{\mathrm{A},1})||Q(\hat{r}_{\mathrm{A},2})||\cdots||Q(\hat{r}_{\mathrm{A},N}) \tag{45}$$

Here, ($CFO\text{-}ID_{\mathrm{A}}$, $IQI\text{-}ID_{\mathrm{A}}$) is the PHY-ID of SN-A. P_A is defined by

$$P_A = h(PubK_A)||f(PubK_A, CFO\text{-}ID_{\mathrm{A}}, IQI\text{-}ID_{\mathrm{A}}) \tag{46}$$

where $h(\cdot)$ produces a hashed $PubK_A$ with a fixed length of V, and $f(\cdot)$ is a user-defined function. In contrast to the hash function, the requirement of $f(\cdot)$ is that it can be inverted to uniquely calculate the public key as

$$PubK_A = f^{-1}(\bar{P}_A, CFO\text{-}ID_{\mathrm{A}}, IQI\text{-}ID_{\mathrm{A}}) \tag{47}$$

where $\bar{P}_A$ denotes P_A with the first V bits eliminated, i.e., $h(PubK_A)$ eliminated. Eq. (47) ensures that the correct $PubK_A$ will be produced if and only if the correct PHY-ID of SN-A is used. Like the email address of a user in IBC, our PHY-ID, which is uniquely associated with SN-A, is reliable during the time scale of E2E authentications, and can be publicly obtained from the KGC by any authorized user for verification. In addition, this public key protection relies on the verification of the physical possession of hardware-level CFO and IQI rather than on the intractability of eq. (46). Thus, $f(\cdot)$ can be lightweight to avoid high computational cost.

In our method, DN receives $PubK_A$ from KGC in the form of P_A. Upon attaining $PubK_A$ using (47), DN can compute $h(PubK_A)$ and compare the result with the received $h(PubK_A)$ (i.e., the first V bits of P_A) to further guarantee the integrity of the obtained $PubK_A$.

Algorithm 2 Registration Procedures

1: SN-A sends **d** to all N SCNs.
2: Each SCN_i obtains $(\hat{\varepsilon}_{\mathrm{A},i}, \hat{\mu}_{\mathrm{A},i})$ of SN-A using (12) and Algorithm 1.
3: SCN_i adds $(\hat{\varepsilon}_{\mathrm{A},i}, \hat{\mu}_{\mathrm{A},i})$ into its whitelist $\mathbf{W}_i$, and sends $(\hat{\varepsilon}_{\mathrm{A},i}, \hat{\mu}_{\mathrm{A},i})$ to AP.
4: AP quantizes $(\hat{\varepsilon}_{\mathrm{A},i}, \hat{\mu}_{\mathrm{A},i})$ into Q_i using (30) and (36), and sends Q_i to KGC.
5: KGC generates $PvtK_A$ and $PubK_A$ using existing asymmetric key mechanism, and sends $PvtK_A$ to SN-A.
6: KGC applies Q_i into PHY-IBC key protection using (44), (45) and (46).
7: End of the algorithm.

C. ALGORITHM OF THE REGISTRATION PROCEDURE

Based on the proposed CFO/IQI estimation, quantization, and PHY-IBC key protection, the procedures of registration phase are given by Algorithm 2.

VI. TWO-STEP AUTHENTICATION PHASE

After the registration of SN-A, any entity that claims to be SN-A should be examined by our two-step authentication

scheme. In this section, we assume that an SN-B sends sensed data and claims $ID_{SN\text{-}A}$ (an upper-layer identity of SN-A) to DN. In this case, DN must determine whether this SN-B is SN-A, as it claims.

A. STEP 1: PRELIMINARY PHY AUTHENTICATION WITH THE AID OF SCN_i

In practice, the upper-layer $ID_{SN\text{-}A}$ (e.g., media access control address) is usually programmable. Once detected, a sophisticated attacker can easily modify its $ID_{SN\text{-}A}$ to launch the spoofing attack again. However, it is practically impossible to arbitrarily change the hardware-level PHY-ID in a short time. In most cases, different devices' CFO and IQI parameters are sufficiently different. Therefore, it is more efficient to first exclude the easily detectable ISNs by verifying this SN-B's $(\hat{\varepsilon}_{\mathrm{B},i}, \hat{\mu}_{\mathrm{B},i})$ at SCN_i before executing the time-consuming E2E cryptography at DN.

It is assumed that N SCNs can receive the data that are sent by SN-B. We select SCN_i in the main link (e.g., SCN_1/AP in the case of Fig.1) for Step 1 authentication. This SCN_i first estimates this SN-B's $(\hat{\varepsilon}_{\mathrm{B},i}, \hat{\mu}_{\mathrm{B},i})$ based on the received signals. Then, SCN_i uses the claimed $ID_{SN\text{-}A}$ as an index to find $(\hat{\varepsilon}_{\mathrm{A},i}, \hat{\mu}_{\mathrm{A},i})$ of SN-A, which has been registered in $\mathbf{W}_i$. The differences between $(\hat{\varepsilon}_{\mathrm{A},i}, \hat{\mu}_{\mathrm{A},i})$ and $(\hat{\varepsilon}_{\mathrm{B},i}, \hat{\mu}_{\mathrm{B},i})$ can be measured by the normalized mean square error (NMSE), which is defined by

$$NMSE_{\mathrm{CFO}} = \frac{(|\hat{\varepsilon}_{\mathrm{A},i}| - |\hat{\varepsilon}_{\mathrm{B},i}|)^2}{|\hat{\varepsilon}_{\mathrm{A},i}|^2} \tag{48a}$$

$$NMSE_{\mathrm{IQI}} = \frac{(|\hat{\mu}_{\mathrm{A},i}| - |\hat{\mu}_{\mathrm{B},i}|)^2}{|\hat{\mu}_{\mathrm{A},i}|^2}. \tag{48b}$$

Alternatively, $\hat{\mu}_{\mathrm{A/B},i}$ can be replaced by $\hat{\nu}_{\mathrm{A/B},i}$ in (48b) to obtain the NMSE of $\nu_{\mathrm{A},i}$. Based on (10) and (48b), the NMSE of $\mu_{\mathrm{A},i}$ or $\nu_{\mathrm{A},i}$ is equal to the NMSE of the corresponding k_j, where $j = 1, 2, 3, 4$.

Setting t_{CFO} and t_{IQI} as the predefined acceptable NMSE rates, a binary hypothesis testing of CFO dimension can be given by

$$NMSE_{\mathrm{CFO}} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} t_{\mathrm{CFO}} \tag{49}$$

where $\mathcal{H}_0$ denotes that SN-A and SN-B have the same CFO feature, and $\mathcal{H}_1$ denotes SN-B$\neq$SN-A. Similarly, the IQI dimension verifies SN-B by

$$NMSE_{\mathrm{IQI}} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} t_{\mathrm{IQI}}. \tag{50}$$

In case that two different SNs occasionally have similar CFO or IQI due to the limited range of RF features, we consider SN-B=SN-A only if both (49) and (50) claim $\mathcal{H}_0$.

The traditional likelihood ratio test (LRT), such as used in [11], is not adopted in our Step 1 authentication for the sake of reducing unnecessary complexity. Firstly, due to the uncertain iteration numbers that are used in the CFO and IQI estimation algorithm, general closed-form expressions of likelihood functions of $(\hat{\varepsilon}_{\mathrm{A/B},i}, \hat{\mu}_{\mathrm{A/B},i})$ are unavailable. Secondly, in our two-step authentication design, Step 1 only plays the role of a preliminary authentication to quickly exclude the easily detectable adversaries in a lightweight processing manner. In this case, we can conservatively set larger values for t_{CFO} and t_{IQI} since more restrictive cryptography-based Step 2 authentication can be performed thenceforth.

Additionally, the execution of Step 1 authentication is optional in our method. For example, we assume that the presence of an attacker has been detected and this attacker's CFO and IQI have been recorded. In practice, this same attacker may simply modify its upper-layer $ID_{SN\text{-}A}$ in order to impersonate another LSN. In this case, the Step 1 authentication at SCN_i can be enabled to quickly detect this attacker again, thereby avoiding the time cost of E2E authentication processing. In other cases, Step 1 can be disabled.

Finally, if the current SN-B passes Step 1 authentication, Step 2 authentication will be executed; otherwise, SCN_i terminates the authentication and abandons the sensed data of SN-B.

B. STEP 2: CRYPTOGRAPHY-BASED AUTHENTICATION WITH THE PHY PROTECTED KEY

Since our PHY-aided method is designed to seamlessly integrate with the general asymmetric cryptography-based authentication, we refer to the typical one-way hash digital signature scheme to describe the procedures of Step 2 authentication.

As shown in Fig.4, the SN-B under examination uses its private key $PvtK_B$ to generate the signature and sends M_1 (the signature combined with the original data) to DN. As mentioned previously, SCN_1/AP performs Step 1 authentication based on the analysis of M_1. If Step 1 is passed, AP collects all N $(\hat{\varepsilon}_{\mathrm{B},i}, \hat{r}_{\mathrm{B},i})$ from SCN_i, quantizes $(\hat{\varepsilon}_{\mathrm{B},i}, \hat{r}_{\mathrm{B},i})$, and calculates $(CFO\text{-}ID_{\mathrm{B}}, IQI\text{-}ID_{\mathrm{B}})$ using (44) and (45), as performed in the registration phase. After that, $M_2 = M_1||CFO\text{-}ID_{\mathrm{B}}||IQI\text{-}ID_{\mathrm{B}}$ is sent to DN.

Upon receiving M_2, DN extracts $(CFO\text{-}ID_{\mathrm{B}}, IQI\text{-}ID_{\mathrm{B}})$, and requests P_A from KGC. Substituting $\bar{P}_A$, $CFO\text{-}ID_{\mathrm{B}}$, and $IQI\text{-}ID_{\mathrm{B}}$ into (47), DN can get a $PubK_{A/B}$. Then, the original data are extracted and hashed to obtain digest D_1 using $h(\cdot)$. Meanwhile, $PubK_{A/B}$ is applied to the signature to generate digest D_2. Under the premise that only SN-A has the correct $PvtK_A$ and only SN-A's (ε_A, μ_A) can result in $PubK_{A/B} = PubK_A$, the readability of D_2 and $D_1 = D_2$ can guarantee that SN-A = SN-B as it claimed, and the integrity of the received message contents is confirmed. Otherwise, we claim that the current SN-B is not the pre-registered SN-A and, thus, the received data must be rejected.

VII. SYSTEM EVALUATION

In this section, we first present the computer simulation results of our proposed authentication in terms of the NMSE estimation performance, probability of detection, correct authentication probability, and authentication processing time. Then, we demonstrate the security strength

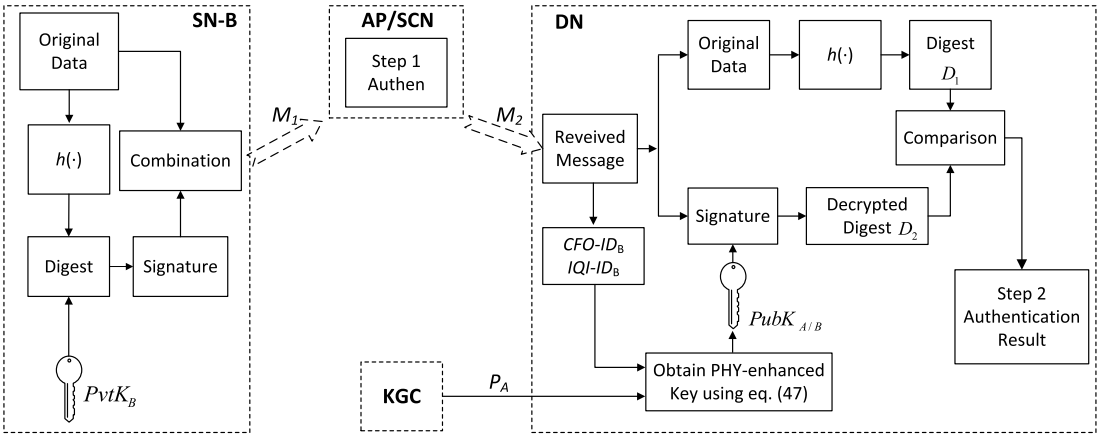


FIGURE 4. Procedures of authentication using a typical one-way hash digital signature with PHY-enhanced key.

enhancement gained by integrating our PHY-aided method into cryptography-based authentication schemes.

A. SIMULATION RESULTS

We consider an OFDM system for the D2D link from SN to SCNs. In every transmission, the QPSK training signal with $K = 512$ sub-carriers is passed through the multi-path channel. The elements of channel vector $\mathbf{h}_i$ are i.i.d. complex circularly symmetric Gaussian random variables as $h_i \sim CN(0, 2)$ with $L = 8$, and the receiving noise follows $w_{z_i} \sim CN(0, \sigma^2)$. SNR is defined as SNR=$10\log_{10}(\frac{P}{\sigma^2})$. Referring to the ranges of the CFO and IQI parameters that are used in [36], we consider $\varepsilon_{\mathrm{A},i}$, $\theta_{\mathrm{tx/rx}}$ and $\alpha_{\mathrm{tx/rx}}$ to be randomly selected as $\varepsilon_{\mathrm{A},i} \sim [-1,\ 1]$, $\theta_{\mathrm{tx/rx}} \sim [-10°,\ 10°]$, $\alpha_{\mathrm{tx/rx}} \sim [-0.1,\ 0.1]$. k_3 is chosen for the NMSE-based Step 1 process. We define $f(PubK_A, CFO\text{-}ID_{\mathrm{A}}, IQI\text{-}ID_{\mathrm{A}}) = PubK_A + 100CFO\text{-}ID_{\mathrm{A}} + 1000IQI\text{-}ID_{\mathrm{A}}$. ECC is used for the asymmetric key algorithm. Specifically, we consider a prime finite field F_p that is defined by the equation $y^2 = x^3 + ax + b$, where $a, b \in F_p$ satisfy $4a^3 + 27b^2 \neq 0$ [41]. As mentioned earlier, the ECC-based key generation, agreement and management are outside of the scope of our paper and, thus, are not considered. We thereby directly apply the ECC generated key pair ($PubK$ and $PvtK$) in our simulations.

For feasibility purpose, this study considers practically estimated CFO and IQI parameters ($\hat{\varepsilon}_{\mathrm{A},i}$ and $\hat{k}_j, j = 1, 2, 3, 4$) rather than assuming perfectly estimated CFO and IQI. As concluded in Section VI-A, the NMSE of $\mu_{\mathrm{A},i}$ or $\nu_{\mathrm{A},i}$ is equal to the NMSE of the corresponding k_j. Therefore, we show the NMSEs of $\hat{\varepsilon}_{\mathrm{A},i}$ and $\hat{k}_j$ in Fig.5 to evaluate the estimation performance and the performances of (48a) (48b) under $\mathcal{H}_0$. It is observed that the NMSE of $\hat{\varepsilon}_{\mathrm{A},i}$ is less than the NMSE of $\hat{k}_j$ in all simulated cases, which is mainly caused by the accumulated estimation inaccuracies. In our estimation technique, $\hat{\varepsilon}_{\mathrm{A},i}$ is estimated first; thus, its estimation inaccuracies are inevitably incorporated into the IQI estimation process. Besides, IQI estimation involves three LS estimations (i.e., Eq. (17) (22) and (26)) in every iteration of Algorithm 1.

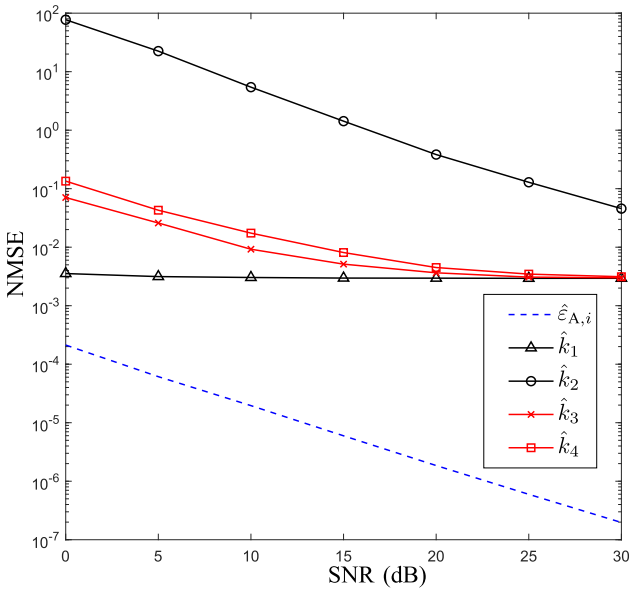


FIGURE 5. NMSE performances of the estimated CFO and IQI parameters under $\mathcal{H}_0$.

All LS estimations inevitably induce additional inaccuracies. Regarding $\hat{k}_1$, $\hat{k}_2$, $\hat{k}_3$ and $\hat{k}_4$, the NMSE of $\hat{k}_2$ is the highest, implying $\hat{k}_2$ is not suitable for authentication. Although $\hat{k}_1$ has the smallest NMSE, it is still an improper choice for authentication, as will be validated in Fig.7. As shown, $\hat{k}_3$ and $\hat{k}_4$ are better choices, and we use $\hat{k}_3$ for Step 1 authentication since its NMSE is slightly less than the NMSE of $\hat{k}_4$ in our case.

We evaluate the detection probability performance P_D, which is defined as the probability of detecting the alternative hypothesis [42]. In Fig. 6, our PHY Step 1 authentication is compared with three other PHY approaches that use either CFO [11] or IQI [12], [43]. Since [43] requires relatively large IQI values for accurate differentiation, it does not perform well in this more challenging simulation with

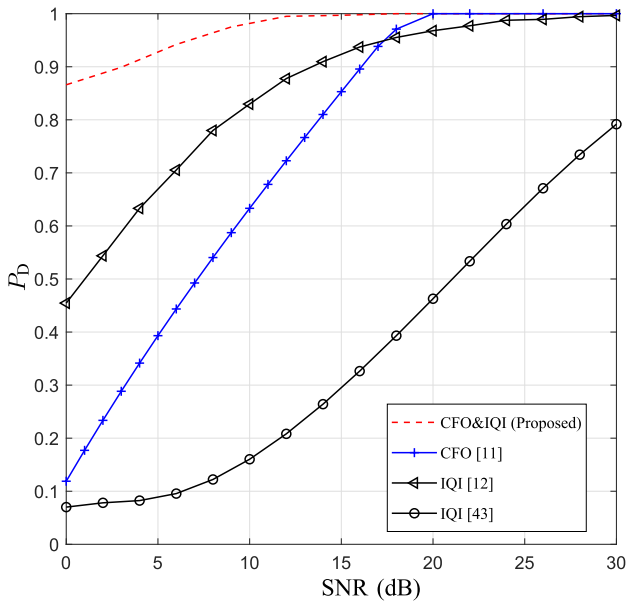


FIGURE 6. Detection probability performance comparison under $t_{\text{CFO}} = 0.5\%$ and $t_{\text{IQI}} = 8\%$.

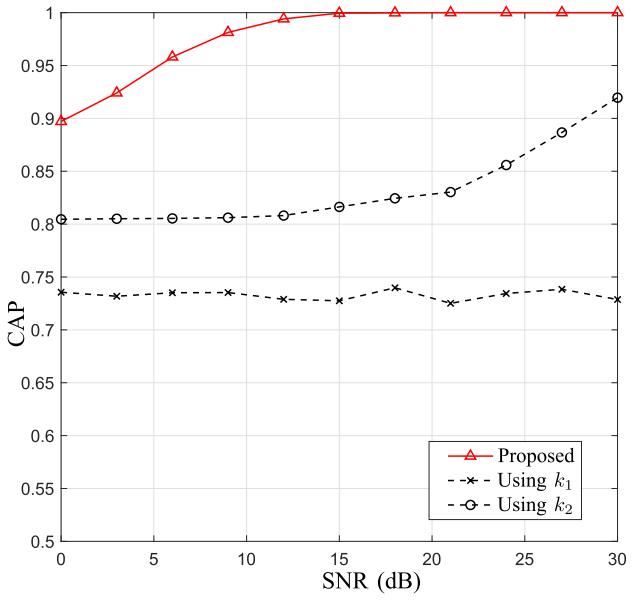


FIGURE 7. Performance in terms of correct authentication probability.

small IQI. Due to the limited ranges of hardware-level CFO and IQI, the accurate detection of the minor CFO/IQI differences is extremely difficult under poor communication conditions (e.g., low SNR). Our P_D outperforms the P_D of all three compared methods, especially in the low SNR regime, which demonstrates the benefit of using our CFO/IQI-based MAMO technique.

The correct authentication probability (CAP) of our Step 1 authentication is evaluated in Fig.7, where CAP is defined as the number of correct ISN and LSN decisions divided by the total number of authentication attempts. We consider 4 LSNs and 1 ISN. In each round of authentication, we select an SN (either LSN or ISN) and accurately claim $\mathcal{H}_0/\mathcal{H}_1$ using (49) and (50). It can be seen that CAP of our method is persistently higher than 90% in all simulated cases. As shown, our proposed method using k_3 is further compared with the cases that use k_1 and k_2. Our CAP is remarkably higher, which confirms our early conclusion that k_1 and k_2 are not suitable for authentication.

The results of PHY entropy derived in Section V-A are simulated in two cases. In case 1 (red dashed curves), we set constant $K_i = L_i = 1000$ for all N SCNs. In case 2 (black solid curves), for each SCN_i, we consider $L_i = i \times 1000$, $K_i = L_i/2$. According to Fig. 8, H_{CFO}, H_{IQI} and H can be boosted by MAMO with larger N and multiple RF features. Additionally, PHY entropy can be adjusted by dynamically changing the number of SCNs (i.e., N) and the number of quantization levels of different SCN_i (i.e., K_i and P_i). Therefore, it is practically possible to use our method to generate the required amount of entropy for E2E security.

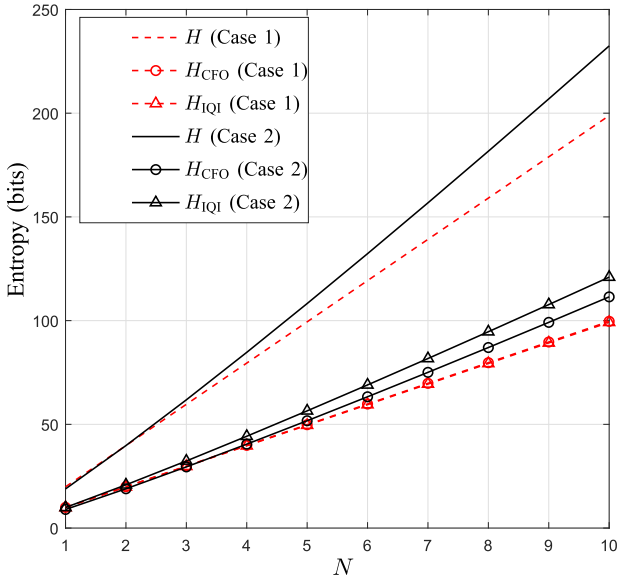


FIGURE 8. PHY entropy of CFO and IQI.

Then, we focus on evaluating the time cost of our Step 1 PHY authentication. Since the important CFO and IQI parameters can be conveniently estimated from any signal that is transmitted by an IoT device (SN), our PHY-aided approach does not require the resource-limited SN to carry out any additional processes except the basic operations that are required by the existing cryptography-based authentication schemes. Therefore, we only need to evaluate the authentication time that is spent by a SCN_i in Step 1 processing. In Fig.9, we compare the average time of performing 1) the mandatory CFO and IQI estimations, 2) our proposed Step 1 PHY authentication, and 3) another traditional IQI-based PHY authentication [12]. Note that the time of our Step 1 method

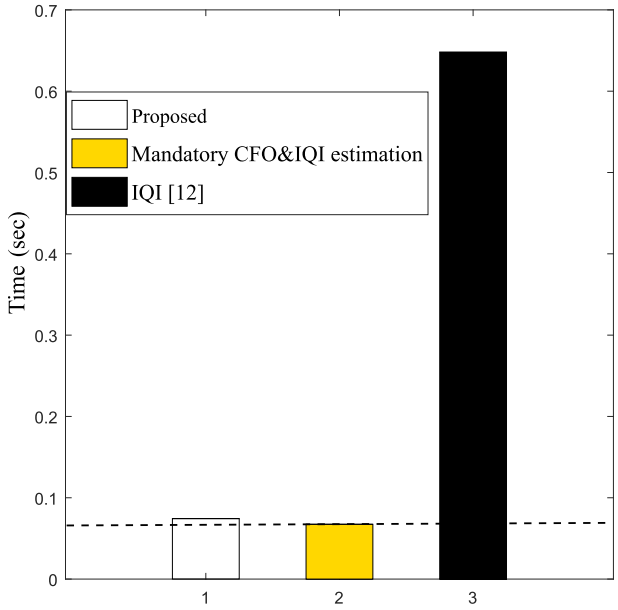


FIGURE 9. Step 1 PHY processing time comparison.

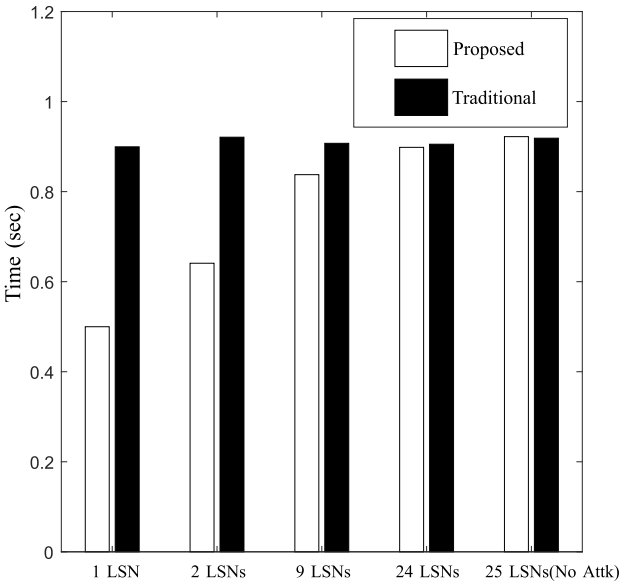


FIGURE 10. Two-step authentication time comparison.

and [12] include the mandatory estimation time plus their individual PHY authentication processing time. As expected, in addition to the necessary estimation time (dashed line), the traditional IQI-based authentication spends much longer time than our method due to the time-consuming LRT (as discussed in Section VI-A). This result confirms the fact that our NMSE-based method does not pose much extra computational complexity, which is suitable for resource-limited IoT devices.

Fig.10 compares the average time spent on completing the proposed two-step authentication and the traditional ECC-based authentication. The number of LSNs gradually increases from 1 to 25 in the five simulated cases. An attacker is present in the first four cases, but absent in the last case. In every authentication round, we randomly select an SN. The possibility of selecting an attacker decreases as the number of LSNs increases. If the attacker is selected, this attacker will impersonate an LSN (e.g., by claiming upper-layer $ID_{SN\text{-}A}$). Using our two-step method, every selected SN (attacker or LSN) will be first tested by the Step 1 authentication. If Step 1 is passed, our Step 2 authentication with ECC will be executed to further examine the selected SN. While, in traditional method, every selected SN will be directly examined by the ECC-based authentication. Fig.10 demonstrates that the average time cost of the traditional method is almost constant, which equals to the average time spent executing ECC. Although the average time cost of the proposed method is slowly increasing, it is always less than that of the traditional method if the attacker is present. This time reduction is achieved since the attacker can be quickly detected by Step 1 in most cases; thus, the time-consuming E2E encryption processes in Step 2 can be avoided. This result also implies our method is more capable of handling the authentication of a small group of devices (small number of SNs) in terms of time cost, for example, in the context of small cells in 5G. In the last case (absence of an attacker), the Step 2 of our method cannot be avoided, and thus the time of our method is slightly longer than traditional method. As mentioned earlier, the execution of optional Step 1 can be elaborately designed in the consideration of the real situation to attain higher time efficiency. For instance, if the presence of an attacker has been detected earlier, then our Step 1 can be enabled temporarily to quickly prevent the same attacker from reappearing in the future. In doing so, the time-consuming E2E data delivery can be even avoided. If unaware of the attacker's presence, the Step 1 can be disabled at any time.

B. ANALYSIS OF THE SECURITY STRENGTH ENHANCEMENT

This subsection evaluates the security strength enhancement gained by using our PHY-aided authentication in terms of resisting various types of impersonation attacks. We consider an attacker who is trying to impersonate the legitimate SN-A in order to communicate with DN. It is assumed that SCNs, KGC and DN are trusted, the link between AP–DN and the process of registration phase are secure, and the Step 1 authentication is enabled.

Case 1: It is assumed that an attacker can passively eavesdrop on messages that are transmitted by SN-A without being detected. To impersonate the legitimate SN-A, this attacker launches a replay attack by sending the intercepted message to SCN_i. However, SCN_i stealthily extracts the CFO and IQI parameters from the analog signal rather than actively requesting any pre-shared secret to be embedded into the message for authentication. Due to attacker's CFO and IQI cannot

be simultaneously the same as SN-A's CFO and IQI, this attacker will be quickly detected by the Step 1 examination.

Case 2: We assume that, occasionally, an attacker has a similar PHY RF feature to SN-A. To prevent this, our MAMO-based method exploits 3-dimensional RF features: CFO, I/Q amplitude mismatch and I/Q phase shift mismatch. Given the impossibility of finding two IoT devices with all 3 identical RF features in a short time duration, our Step 1 authentication is reliable.

Case 3: Conventionally, the key step in breaking through a cryptography-based authentication system is the determination of credentials, such as determining the encryption keys and certificate. As the main advantage of our PHY-IBC, our method eliminates the need for a certificate mechanism. Therefore, the attacker has to try to compromise the private key of SN-A (i.e., $PvtK_A$) or spoof the public key of SN-A ($PubK_A$) as follows:

- *Compromising* $PvtK_A$*:* It is assumed that an attacker can intercept $PvtK_A$ or compromise the length-shortened $PvtK_A$ (e.g., by guessing or exhaustive search). As a result, this attacker with correct $PvtK_A$ will be determined to be legitimate by the traditional cryptography-based authentication.
- *Spoofing* $PubK_A$*:* It is assumed that an attacker's key pair is ($PvtK_B$, $PubK_B$). This attacker cannot compromise $PvtK_A$, but, alternatively, can send its $PubK_B$ to DN. In traditional cryptography-based authentication, the attacker will win if DN trusts $PubK_B$. This is because the signature that is used for authentication can be generated by attacker's $PvtK_B$.

In our system, when this attacker tries to communicate with DN, the SCN_i can directly obtain this attacker's CFO and IQI parameters, which are directly associated with the RF hardware of the attacker. In collaboration with SCN_i, DN can generate ($CFO\text{-}ID_{\rm B}$, $IQI\text{-}ID_{\rm B}$). An incorrect public key ($PubK_C$) must be produced by substituting ($CFO\text{-}ID_{\rm B}$, $IQI\text{-}ID_{\rm B}$) in (47) since $CFO\text{-}ID_{\rm A} \neq CFO\text{-}ID_{\rm B}$ and $IQI\text{-}ID_{\rm A} \neq IQI\text{-}ID_{\rm B}$. Note that $PubK_A \neq PubK_B \neq PubK_C$. Using $PubK_C$, DN cannot correctly decrypt the signature to obtain the readable message D_2; thus, the impersonation attacker will be detected. Consequently, our authentication is secure against the above-mentioned *Compromising* $PvtK_A$ attack and *Spoofing* $PubK_A$ attack.

Case 4: We assume that an attacker tries to determine SN-A's PHY-ID=($CFO\text{-}ID_{\rm A}$, $IQI\text{-}ID_{\rm A}$). To this end, the attacker has to figure out how to compute the MAMO-based ($CFO\text{-}ID_{\rm A}$, $IQI\text{-}ID_{\rm A}$). However, the attacker does not know 1) the values of M and N; 2) which N SCNs out of which M CNs are used; and 3) what quantization rules are separately used for different SCN_i (e.g., K_i and P_i are unknown). Furthermore, N, K_i and P_i can be dynamically adjusted. More importantly, PHY-ID is generated based on direct observations of the signals that are transmitted by the impersonation attacker, which can inherently prevent upper-layer computation-based attacks. Consequently, our PHY-ID is secure.

In summary, the proposed PHY-aided Step 1 authentication can achieve satisfactory P_D, CAP, and time efficiency. PHY-aided Step 2 authentication can increase the resistance to various impersonation attacks.

C. DISCUSSION

The above results demonstrate that the proposed PHY-aided technique can be applied in conventional asymmetric cryptography-based authentication for performance enhancement. In practice, a cryptographic system needs to perform key update and revocation. In addition, the SCNs may leave the network. This subsection discusses the performance of our authentication scheme when encountering these issues. Please keep in mind that this study does not change the existing encryption key management mechanism.

1) KEY REVOCATION

Key revocation is one of the critical concerns of IBC. For instance, the public key is associated with the thumbprint or the email address of a user. If the corresponding private key is lost or compromised, the key pair revocation may cause the thumbprint/email of this user to no longer be usable. To solve this problem, IBC requires regular expiration of the keys, e.g., concatenating a timestamp in the public key as *BoB@email.com||Current Year*.

In our method, the public key $PubK_A$ is protected in the form of P_A using IQI and CFO (i.e., using $CFO\text{-}ID_{\rm A}$ and $IQI\text{-}ID_{\rm A}$ in Eq. (44) (45)). Thus, it can inherently meet the key revocation requirement.

- First, revoking ($PvtK_A$, $PubK_A$) will not abolish the use of the SN-A-associated ($CFO\text{-}ID_{\rm A}$, $IQI\text{-}ID_{\rm A}$). In practice, we can obtain an updated P_A by applying a newly generated $PubK_A$ and ($CFO\text{-}ID_{\rm A}$, $IQI\text{-}ID_{\rm A}$) into (46) after the key revocation.
- Second, our P_A already has the expiration feature. Although extremely slow, the hardware-level RF parameters are time-varying due to, for example, circuit aging. This makes P_A and keys automatically expire when the changes in the CFO and IQI parameters exceed the corresponding quantization intervals. Moreover, we can actively expire P_A by adjusting the quantization rules, for example, by changing K_i and P_i. In addition, registration (Algorithm 2) can be periodically performed for SN-A to handle the slight circuit aging.

2) SEAMLESS INTEGRATION WITH EXISTING KEY UPDATE

The proposed method does not interfere with existing key management mechanism. We consider that the IoT device (SN-A) holds a new $PvtK_A$ after the key update. Our method requires that SN-A with any new key should be registered again using Algorithm 2 to update the PHY-ID and P_A.

3) DISASSOCIATION OF SCN

The disassociation of an SCN_i will not break our PHY-aided authentication. If an SCN_i leaves the network, we need to update ($CFO\text{-}ID_{\rm A}$, $IQI\text{-}ID_{\rm A}$) by removing $Q(\hat{\varepsilon}_{{\rm A},i})$ and

$Q(\hat{r}_{A,i})$ from Eq. (44) and (45), respectively. Then, new P_A can be computed with the updated ($CFO\text{-}ID_A$, $IQI\text{-}ID_A$) using (46).

VIII. CONCLUSION AND FUTURE WORK

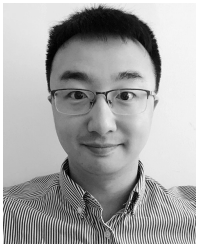
This paper has proposed a PHY-aided E2E IoT device authentication. With the aid of collaborative nodes, our method generates a PHY-ID, which is composed of the RF CFO and IQI features of an IoT device. We seamlessly integrate this PHY-ID with existing, well-established asymmetric cryptography-based authentication schemes. The MAMO and PHY-IBC techniques are proposed for further enhancing the authentication performance. Evaluation results show increased detection probability, correct authentication probability, satisfactory time efficiency, and enhanced security strength, which demonstrates the advantages of using our PHY-aided cross-layer design. Compared to the PUF-based authentication that requires the hardware-level ICs production/installation/retrofit and the CRP related processes, our method does not impose any implementation overhead on the resource-constrained IoT devices. Using PHY-IBC technique, our method achieves strong resistance to the upper-layer computation-based impersonation attacks.

In our future research, we intend to fully exploit the computing resources of collaborative edge nodes to design an optimal PHY entropy-based authentication scheme for IoT security.

REFERENCES

[1] J. Singh, T. Pasquier, J. M. Bacon, H. Ko, and D. Eyers, "Twenty security considerations for cloud-supported Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 269–284, Jul. 2016.
[2] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 408–417, Jun. 2016.
[3] T. Kothmayr, C. Schmitt, W. Hub, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2710–2723, May 2013.
[4] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *Proc. Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 2728–2733.
[5] D. He and S. Zeadally, "An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 72–83, Feb. 2015.
[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.
[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[8] M. Alimomeni and R. Safavi-Naini, "Guessing secrecy," in *Information Theoretic Security*. Berlin, Germany: Springer, 2012.
[9] V. Va and R. W. Heath, Jr., "Basic relationship between channel coherence time and beamwidth in vehicular channels," in *Proc. IEEE 82nd Veh. Technol. Conf.*, Sep. 2015, pp. 1–5.
[10] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future development," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.
[11] W. Hou, X. Wang, and J.-Y. Chouinard, "Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 3559–3563.
[12] P. Hao, X. Wang, and A. Behnad, "Relay authentication by exploiting I/Q imbalance in amplify-and-forward system," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 613–618.
[13] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. IEEE Mil. Commun. Conf.*, Nov. 2011, pp. 538–542.
[14] J. R. Wallrabenstein, "Practical and secure IoT device authentication using physical unclonable functions," in *Proc. IEEE Int. Conf. Future Internet Things Cloud*, Aug. 2016, pp. 99–106.
[15] W. Che, F. Saqib, and J. Plusquellic, "PUF-based authentication," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2015, pp. 337–344.
[16] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.
[17] N. N. Dao, Y. Kim, S. Jeong, M. Park, and S. Cho, "Achievable multi-security levels for lightweight IoT-enabled devices in infrastructureless peer-aware communications," *IEEE Access*, vol. 5, pp. 26743–26753, 2017.
[18] P. Hao and X. Wang, "A PHY-aided secure IoT healthcare system with collaboration of social networks," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, Sep. 2017, pp. 1–6.
[19] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. ACM Int. Conf. Mobile Comput. Netw. (MobiCom)*, 2008, pp. 116–127.
[20] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong, "Efficient online/offline identity-based signature for wireless sensor network," *Int. J. Inf. Secur.*, vol. 9, no. 4, pp. 287–296, Aug. 2010.
[21] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: An identity-based cryptography approach," in *Proc. 1st ACM Conf. Wireless Netw. Secur.*, Jul. 2008, pp. 148–153.
[22] P. Y. Ting, J. L. Tsai, and T. S. Wu, "Signcryption method suitable for low-power IoT devices in a wireless sensor network," *IEEE Syst. J.*, to be published.
[23] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171–4182, Jun. 2016.
[24] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.
[25] D. Chen *et al.*, "S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88–100, Feb. 2017.
[26] A. C. Polak, C. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1469–1479, Aug. 2011.
[27] R. L. Filler and J. R. Vig, "Long-term aging of oscillators," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 40, no. 4, pp. 387–394, Jul. 1993.
[28] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. Berlin, Germany: Springer, 2000.
[29] B. Narasimhan, D. Wang, S. Narayanan, H. Minn, and N. Al-Dhahir, "Digital compensation of frequency-dependent joint Tx/Rx I/Q imbalance in OFDM systems under high mobility," *IEEE J. Sel. Topics Signal Process.*, vol. 3, no. 3, pp. 405–417, Jun. 2009.
[30] P. Kiss and V. Prodanov, "One-tap wideband I/Q compensation for zero-IF filters," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 6, pp. 1062–1074, Jun. 2004.
[31] P. Murphy, "Design, implementation and characterization of a cooperative communications system," Ph.D. dissertation, Dept. Elect. Comput. Eng., Rice Univ., Houston, TX, USA, 2010.
[32] J. Li, M. Matthaiou, and T. Svensson, "I/Q imbalance in AF dual-hop relaying: Performance analysis in Nakagami-*m* fading," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 836–847, Mar. 2014.
[33] Y. Zou, M. Valkama, and M. Renfors, "Digital compensation of I/Q imbalance effects in space-time coded transmit diversity systems," *IEEE Trans. Signal Process.*, vol. 56, no. 6, pp. 2496–2508, Jun. 2008.
[34] H. Minn, N. Al-Dhahir, and Y. Li, "Optimal training signals for MIMO OFDM channel estimation in the presence of frequency offset and phase noise," *IEEE Trans. Commun.*, vol. 54, no. 10, pp. 1754–1759, Oct. 2006.
[35] P. H. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Trans. Commun.*, vol. 42, no. 10, pp. 2908–2914, Oct. 1994.
[36] Y.-H. Chung and S.-M. Phoong, "Joint estimation of I/Q imbalance, CFO and channel response for MIMO OFDM systems," *IEEE Commun. Lett.*, vol. 58, no. 5, pp. 1485–1492, May 2010.

[37] A. Tarighat, R. Bagheri, and A. H. Sayed, "Compensation schemes and performance analysis of IQ imbalances in OFDM receivers," *IEEE Trans. Signal Process.*, vol. 53, no. 8, pp. 3257–3268, Aug. 2005.
[38] W. Hou and M. Jiang, "Enhanced joint channel and IQ imbalance parameter estimation for mobile communications," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1392–1395, Jul. 2013.
[39] F. Horlin and A. Bourdoux, *Digital Compensation for Analog Front-Ends: A New Approach to Wireless Transceiver Design*. Hoboken, NJ, USA: Wiley, 2008.
[40] Y. Xiong, N. Wei, Z. Zhang, B. Li, and Y. Chen, "Channel estimation and IQ imbalance compensation for uplink massive MIMO systems with low-resolution ADCs," *IEEE Access*, vol. 5, pp. 6372–6388, 2017.
[41] K.-H. Yeh, "A secure IoT-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10288–10299, Dec. 2016.
[42] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*, vol. 2. Upper Saddle River, NJ, USA: Prentice-Hall, 1998.
[43] H. Li, X. Wang, and Y. Zou, "Exploiting transmitter I/Q imbalance for estimating the number of active users," in *Proc. IEEE Conf. Global Commun. (GLOBECOM)*, Dec. 2013, pp. 3318–3322.



PENG HAO (S'09–M'16) received the B.S. degree from Qingdao University, China, the M.Sc. degree from Shandong University, China, and the Ph.D. degree in electrical and computer engineering from the University of Western Ontario, London, ON, Canada.

He is currently a Post-Doctoral Associate at the University of Western Ontario. His research interests include wireless communications security, Internet of Things, 5G networks, cloud/edge computing, and eHealth. He has been involved in a number of IEEE conferences in different roles such as the Reviewer, Session Chair, and the Technical Program Co-Chair. From 2014 to 2015, he served as the Treasurer for the IEEE Young Professionals (London). He serves as a Regular Reviewer for several IEEE journals, including the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE WIRELESS COMMUNICATIONS LETTERS, and the IEEE ACCESS.

XIANBIN WANG (S'98–M'99–SM'06–F'17) received the Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2001. He is currently a Professor and the Tier-I Canada Research Chair with the University of Western Ontario, Canada.

From 2002 to 2007, he was a Research Scientist/Senior Research Scientist with the Communications Research Centre Canada. From 2001 to 2002, he was a System Designer at STMicroelectronics, where he was responsible for the system design of DSL and Gigabit Ethernet chipsets. He has over 300 peer-reviewed journal and conference papers, in addition to 26 granted and pending patents and several standard contributions. His current research interests include 5G technologies, Internet-of-Things, communications security, machine learning, and locationing technologies.

Dr. Wang is a fellow of the Canadian Academy of Engineering and an IEEE Distinguished Lecturer. He has received many awards and recognitions, including the Canada Research Chair, the CRC President's Excellence Award, the Canadian Federal Government Public Service Award, the Ontario Early Researcher Award, and five IEEE Best Paper Awards. He was involved in many IEEE conferences including the GLOBECOM, ICC, VTC, PIMRC, WCNC, and CWIT, in different roles such as the Symposium Chair, Tutorial Instructor, Track Chair, Session Chair, and the TPC Co-Chair. He currently serves as an Editor/Associate Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON BROADCASTING, and the IEEE TRANSACTIONS ONVEHICULAR TECHNOLOGY. He was also an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2007 to 2011, and the IEEE WIRELESS COMMUNICATIONS LETTERS from 2011 to 2016.

WEIMING SHEN (M'98–SM'02–F'12) received the B.S. and M.S. degrees from Northern (Beijing) Jiaotong University, China, and the Ph.D. degree in system control from the University of Technology of Compiègne, France. He is currently the Principal Research Scientist at the National Research Council Canada, and also an Adjunct Professor with the University of Western Ontario, Canada.

He has published several books and over 450 papers in scientific journals and international conferences. His work has been cited over 11 000 times with an h-index of 49. His research interests include agent-based collaboration technology and applications, Internet of Things, and big data analytics. He is a Fellow of the Engineering Institute of Canada. He is a Distinguished Lecturer of the IEEE Systems, Man, and Cybernetics Society.