

Access-based Lightweight Physical Layer Authentication for the Internet of Things Devices

Saud Khan, *Student Member, IEEE*, Chandra Thapa, *Member, IEEE*, Salman Durrani, *Senior Member, IEEE*, and Seyit Camtepe, *Senior Member, IEEE*

Abstract—Physical-layer authentication is a popular alternative to the conventional key-based authentication for internet of things (IoT) devices due to their limited computational capacity and battery power. However, this approach has limitations due to poor robustness under channel fluctuations, reconciliation overhead, and no clear safeguard distance to ensure the secrecy of the generated authentication keys. In this regard, we propose a novel, secure, and lightweight continuous authentication scheme for IoT device authentication. Our scheme utilizes the inherent properties of the IoT devices’ transmission model as its source for seed generation and device authentication. Specifically, our proposed scheme provides continuous authentication by checking the access time slots and spreading sequences of the IoT devices instead of repeatedly generating and verifying shared keys. Due to this, access to a coherent key is not required in our proposed scheme, resulting in the concealment of the seed information from attackers. Our proposed authentication scheme for IoT devices demonstrates improved performance compared to the benchmark schemes relying on physical channels. Our empirical results find a near threefold decrease in the misdetection rate of illegitimate devices and close to zero false alarm rate in various system settings with varied numbers of active devices up to 200 and signal-to-noise ratio from 0 dB to 25 dB. Our proposed authentication scheme also has a lower computational complexity of at least half the computational cost of the benchmark schemes based on support vector machine and binary hypothesis testing in our studies. This further corroborates the practicality of our scheme for IoT deployments.

Index Terms—Security of internet of things, lightweight authentication.

I. INTRODUCTION

Internet of Things (IoT) devices are increasingly indispensable to modern society, industry, and governments [2]. These devices are expected to increase from 14 billion in 2022 to 27 billion in 2025 [3]. Moreover, these devices will form an integral part of future networks, including 6G [4]. However, the security of these widely used IoT devices is an increasingly essential issue [5].

IoT devices usually connect to a network through an access point (AP). The conventional approach to establish secure

communications between IoT devices and AP is to generate a shared secret key by exploiting the reciprocity of the random fading channel [6], [7]. Herein, the IoT devices measure highly correlated wireless channel characteristics (*e.g.*, channel impulse responses, or received signal strengths) and use them as shared random sources to generate a shared key. However, the low-cost and often resource-constrained IoT devices cannot facilitate physical-channel probing for a shared key generation due to the limited resources. Instead, these IoT devices rely on intermittent transmissions, which makes them highly susceptible to adversarial attacks [8].

Besides, IoT devices perform sporadic transmission to save energy. Considering sporadic transmission and the massive number of IoT devices in the future network, the non-orthogonal multiple access (NOMA) transmission protocols, which overlap multiple IoT devices over a single radio resource block, are envisioned as a potential solution [2], [9]. Though the sporadic transmission in NOMA enables IoT devices to transmit for extended periods, it also negates the suitability of conventional shared key generation schemes for authentication due to their inherent complexity and reliance on shared key updates. As a result, there can be potential adversaries with abundant opportunities for certain attacks, such as spoofing attacks and eavesdropping [10], [11].

Existing methods, such as upper-layer security protocols, suffer from high computational overhead [12]. Conversely, lightweight options are available, but these often rely on physical channel attributes [13], [14] and are unreliable in the presence of variations and noises. Furthermore, channel probing is challenging given the resource limitation of the devices. This underscores the need for fast (enabled by continuous authentication mechanism), reliable (no reliance on physical channel attributes), and lightweight authentication mechanisms for IoT devices.

A. Contributions

In this paper, we propose a novel lightweight and continuous authentication scheme for resource-constrained IoT devices by identifying the pre-arranged access time slots and spreading pools of each IoT device, which provides high uncertainties for the spoofers and supplies seamless protections for legitimate communications. In our proposed scheme, the access time slots are pre-agreed between a pair of IoT devices and the AP, which are difficult for the adversaries to predict and do not require additional hardware for implementation [15]. The access time slots are generated using the spreading pools available at the

Saud Khan and Salman Durrani are with the School of Engineering, The Australian National University, Canberra, 2601, Australia (Email: {saud.khan, salman.durrani}@anu.edu.au)

Saud Khan, Chandra Thapa and Seyit Camtepe are with Data61, Commonwealth Scientific and Industrial Research Organization (CSIRO), Sydney, 2122, Australia (Email: {chandra.thapa, seyit.camtepe}@data61.csiro.au)

This research was undertaken with the assistance of resources and services from the National Computational Infrastructure (NCI), which is supported by the Australian Government.

This article will be presented in part at the IEEE GLOBECOM Workshop 2023 [1].

AP and IoT devices. The access time slots for every IoT device are generated independently at the AP and the IoT devices, thereby obeying the grant-free NOMA protocol for a practical massive IoT deployment. If the access time slot and spreading pool of an IoT device are different from the access time slot and spreading pool at the AP, it will be identified as an illegitimate device by the AP. *To our best knowledge, this is the first work to authenticate multiple resource-constrained IoT devices utilizing grant-free NOMA protocol by utilizing their spreading pools and pre-arranged access time slots as the source for authentication.* The main contributions of this work are summarised as follows.

- **Authentication scheme:** We propose a lightweight authentication scheme comprised of four processes: access time slots generation, spreading pool construction, seed generation, and authentication decision. The scheme provides continuous authentication by checking the access time slots and spreading pools of the IoT devices instead of generating and verifying shared keys.
- **Reduced overhead and latency:** The spreading sequences, utilized by the IoT devices as part of the grant-free NOMA transmission protocol, are used as the seed source for access time slot generation and IoT device authentication. Thus, our proposed scheme does not need seed verification and reconciliation processes, which incur massive overhead and latency.
- **Improved authentication performance:** Our results in the misdetection rate of illegitimate devices indicate a nearly threefold improvement, false alarm rate indicates state-of-the-art, and spreading sequence collision rate indicates superior performance in different settings while boasting a lower complexity compared to the benchmark schemes. Furthermore, our proposed scheme does not rely on the physical channel reciprocity assumption, which makes it a suitable authentication scheme for resource-constrained IoT devices.

Paper organization : The rest of this paper is organized as follows. In Section II, we review the related studies of authentication schemes for IoTs. In Section III, we present the system model and the authentication problem. In Section IV, we describe the proposed authentication scheme and provide a detailed description of the different phases of device authentication. In Section V, we derive the performance analysis of the proposed authentication scheme. In Section VI, we present the simulation results to verify the performance gain of the proposed technique. Finally, Section VII concludes the paper.

Notations: Lower and upper case boldface letters are used for vectors and matrices, respectively. The transpose of a vector \mathbf{a} is \mathbf{a}^T . The norm is denoted by $\|\cdot\|$. $\mathbb{C}^{x \times y}$ denotes the complex valued space of size $x \times y$ respectively. \odot , \oslash , and $(\cdot)^\dagger$ denote the Hadamard product, the Hadamard division, and the Moore-Penrose matrix inversion, respectively. Table I summarizes the important symbols used in this work, including the dimensions of vectors and matrices.

II. RELATED WORKS

Considering the adversaries, upper-layer security protocols have been increasingly studied in the literature [12], [16].

TABLE I: Important symbols used in this work.

Variable	Description	Dimension
K	Total number of IoT devices	1×1
N	Total subcarriers	1×1
S	Active number of IoT devices	1×1
J	Number of time slots	1×1
\mathbf{c}	Spreading sequence	$N \times 1$
\mathbf{h}	Channel	$N \times 1$
\mathbf{x}	Transmit signal	$K \times 1$
\mathbf{w}	Gaussian noise	$N \times 1$
\mathbf{y}	Received signal	$N \times 1$
\mathbf{G}	Synthesis of channel vector and spreading sequences	$N \times K$
\mathbf{H}	Channel matrix	$N \times K$
\mathbf{C}	Codebook matrix	$N \times K$
\mathbf{X}	Transmit signal (continuous time slots)	$K \times J$
$\bar{\mathbf{G}}$	Synthesis of channel vector and spreading sequences (continuous time slots)	$N \times K$
\mathbf{W}	Gaussian noise (continuous time slots)	$N \times J$
\mathbf{Y}	Received signal (continuous time slots)	$N \times J$
$\mathbf{\Gamma}$	Authenticated devices' indicator	$K \times J$
$\bar{\mathbf{X}}$	Authenticated devices' data	$K \times J$

However, they are not well suited for resource-constrained IoT devices due to their massive computational overhead and excessive latency. In this regard, low-complexity authentication schemes are desirable for resource-constrained IoT devices, complementing the overall network entropy by introducing additional measures for IoT device authentication in the lower layers [17], [18].

Physical layer security schemes based on keyless authentication [19]–[21] can provide lightweight security to the resource-constrained IoT devices by exploiting the inherent physical-channel attributes and/or device-specific features of IoT devices. By doing so, the overall network entropy can be improved while reducing IoT devices' computational cost and energy consumption. The authors in [19] introduced scheduling policies to utilize the physical channel characteristics for device authentication. The authors in [20] utilized the channel and phase noise of the physical channel between a transceiver pair utilizing multiple antennas for hypothesis testing and device authentication. Similarly, the authors in [21] utilized the correlation of multiple channel impulse responses (CIR) from the physical channel for authentication. Recently, machine learning has also been applied to combine with physical layer authentication schemes to improve the robustness under channel fluctuations [13], [14], [22]. However, the reliance of these techniques on the physical channel for feature extraction results in unreliable authentication performance due to variations and noises present in complex dynamic environments.

In a different approach, to achieve continuous authentication, the authors in [23] used an authentication mechanism to create a learning-based kernel model that utilizes multi-attributes from the physical channel for device authentication. Then, the authors in [15] utilized the multi-attribute design of the physical channel and support vector machine (SVM) to utilize pseudo-random binary access time slots for device authentication. However, due to the time-varying nature of the physical channel, especially in complex dynamic environments, and the low-cost components utilized by the IoT devices, the variations and noise cause unreliable seed

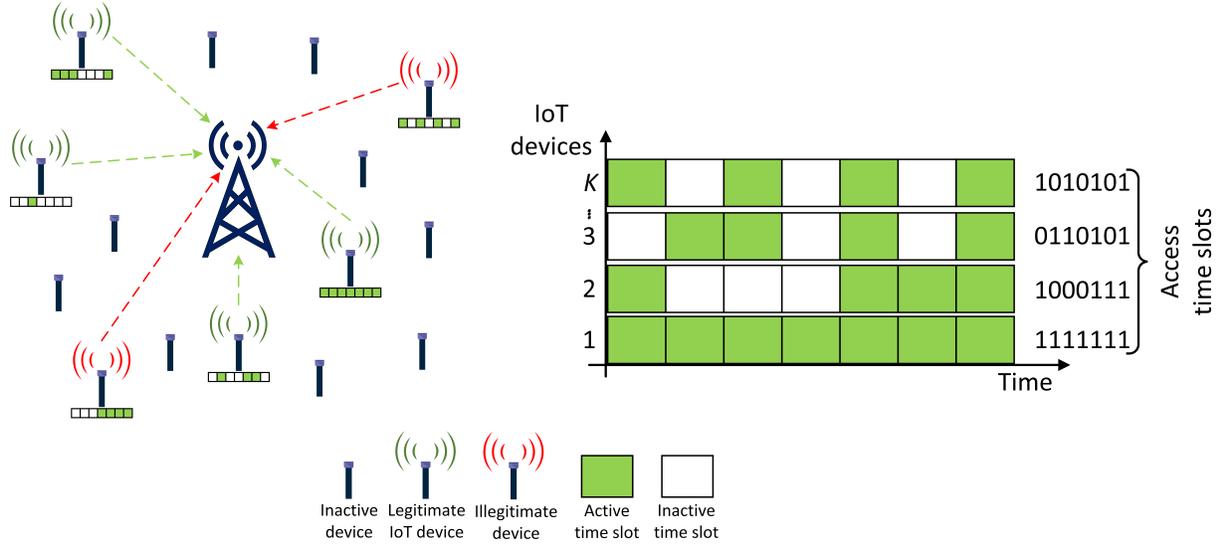


Fig. 1: Illustration of our system model. The transmission between the IoT devices and the AP is carried out by following the pre-agreed access time slots.

acquisition. Additionally, since these works are based on the assumption of physical channel reciprocity, they will incur a high seed mismatch rate due to the half-duplex nature of the resource-constrained IoT devices; this results in multi-staged parity bits for seed reconciliation, which is against the deployment spirit of resource-constrained IoT devices. Moreover, since the IoT devices are resource-constrained, the physical channel probing process cannot be carried out due to the inherent sporadic communication nature of the IoT devices.

In order to overcome the aforementioned challenges, we propose an access-based framework that paves the way for lightweight and continuous authentication tailored for resource-constrained IoT devices.

III. SYSTEM MODEL

In this paper, we consider the scenario where IoT devices wake up sporadically and transmit their data to the AP in a grant-free manner, as depicted in Fig. 1. Thus, we consider a spreading-based uplink grant-free NOMA system comprising of an AP and K IoT devices with limited computing capabilities. The AP has relatively powerful computing capabilities and is at a fixed location. The AP and IoT devices are assumed to be equipped with a single antenna, and their clocks are synchronized¹. We assume that upper-layer security mechanisms are utilized initially to establish system parameters between the AP and IoT devices [22]. During transmission, a subset of the K IoT devices sporadically and randomly become active when they have data to transmit. We consider an overloaded system where the number of resource blocks N is less than the number of IoT devices in a cell, i.e., $N < K$.

¹Practically, clock synchronization can be achieved via methods described in [24]–[26] to achieve energy-efficient communications for IoT devices. However, this is outside the scope of this work.

A. Threat Model

In the system model, as depicted in Fig. 1, we assume that illegitimate devices can be present anywhere in a cell, including in close proximity to legitimate IoT devices, and therefore, their physical channels can be correlated. As a result, the AP can receive transmissions from both legitimate IoT and illegitimate devices, where the illegitimate devices attempt to access the network by conducting spoofing attacks, such as man-in-the-middle attacks and replay attacks. With this in mind, apart from the codebook matrix², we assume that the illegitimate devices utilize the same system parameters and upper-layer signaling as the legitimate IoT devices, as detailed in Table I. We further assume that the illegitimate devices can remain active at all times and can scan the network to learn the transmission pattern of legitimate IoT devices. Thus, illegitimate devices can be resourceful and more computationally capable than legitimate IoT devices.

B. Signal Model

Considering an arbitrary symbol interval, an IoT device randomly wakes up and transmits its complex modulated signal towards the AP, which are independent random variables drawn from a standard symmetric discrete constellation set. After modulation, the transmitted symbol x_k from the k -th IoT device is spread onto a spreading sequence \mathbf{c}_k of length N . The received signal y on the n -th subcarrier at the AP is given as

$$y_n = \sum_{k=1}^K h_{nk} c_{nk} x_k + w_n, \quad (1)$$

where h_{nk} refer to the n -th subcarrier of the k -th IoT device's channel vector $\mathbf{h}_k = [h_{1k}, h_{2k}, \dots, h_{Nk}]^T \in \mathbb{C}^{N \times 1}$,

²Generally, the AP can refresh the codebook matrix in a cell to enhance communication using different methods [27], [28]. However, this is a separate research topic and is, therefore, outside the scope of this work.

c_{nk} refer to the n -th component of the spreading sequence $\mathbf{c}_k = [c_{1k}, c_{2k}, \dots, c_{Nk}]^T \in \mathbb{C}^{N \times 1}$, and w_n is the Gaussian noise on the n -th subcarrier with zero mean and variance σ^2 . By combining the received signals overall N subcarriers, the received signal vector $\mathbf{y} = [y_1, y_2, \dots, y_N]^T \in \mathbb{C}^{N \times 1}$ is given as

$$\mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{w}, \quad (2)$$

where $\mathbf{x} = [x_1, x_2, \dots, x_K]^T \in \mathbb{C}^{K \times 1}$ is the transmitted signal vector for all K devices and $\mathbf{w} = [w_1, w_2, \dots, w_N]^T \in \mathbb{C}^{N \times 1}$ is the noise vector. $\mathbf{G} \in \mathbb{C}^{N \times K}$ is the synthesis of the channel vectors and spreading sequences, given as

$$\mathbf{G} = \mathbf{H} \odot \mathbf{C}, \quad (3)$$

where $\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_K] \in \mathbb{C}^{N \times K}$ is the channel matrix, $\mathbf{C} = [\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_K] \in \mathbb{C}^{N \times K}$ is the codebook matrix, and \odot is the Hadamard product, *i.e.*, $g_{nk} = h_{nk}c_{nk}$.

C. Transmission Model

Different works [29]–[31] have assumed that the active IoT devices remain unchanged in an entire frame. However, in practical grant-free systems, the IoT devices access or leave the system randomly [2]. Moreover, once active, due to the size of their data payload, some IoT devices transmit their data in consecutive time slots. From this, it concurs that the nature of data transmission by IoT devices is generically random and not deterministic. Therefore, we consider a scenario where the IoT devices become active or inactive in different time slots, which is a more practical scenario in 6G IoT applications with sporadic communications. Motivated by this, we can extend the signal model in (2) from a single time slot transmission model to a continuous time-slots transmission model.

The transmitted signals $\mathbf{X} = [\mathbf{x}^{[1]}, \mathbf{x}^{[2]}, \dots, \mathbf{x}^{[J]}] \in \mathbb{C}^{K \times J}$ are recovered from the received signals $\mathbf{Y} = [\mathbf{y}^{[1]}, \mathbf{y}^{[2]}, \dots, \mathbf{y}^{[J]}] \in \mathbb{C}^{N \times J}$ in J continuous time slots, based on the LTE-Advanced standard protocol [32]. Thus, the continuous time-slots transmission model for the j -th time slot is given as

$$\mathbf{y}^{[j]} = \mathbf{G}^{[j]}\mathbf{x}^{[j]} + \mathbf{w}^{[j]}, \quad j = 1, 2, \dots, J, \quad (4)$$

where $\mathbf{G}^{[j]} \in \mathbb{C}^{N \times K}$ is the synthesis of the channel vectors and spreading sequences in the j -th time slot and $\mathbf{w}^{[j]}$ is the equivalent Gaussian noise vector in the j -th time slot.

D. Problem Statement

The sporadic nature of the IoT devices allows the illegitimate devices to impersonate the legitimate IoT devices to spoof the AP and gain access to the core network. Assuming that an IoT device transmits to the AP in the j -th time slot, the objective at the AP is to authenticate the device if the message originated from a legitimate IoT device. In order to achieve this, the AP and the legitimate IoT devices can agree on specific transceiver features or characteristics, which can be used to distinguish legitimate IoT devices from illegitimate devices. Let $\Gamma^{[j]}$ represent the authenticated devices indicator

in the j -th time slot; then, the authentication problem is given as

$$\Gamma^{[j]} = \begin{cases} 1 & \text{if } \mathcal{H}_0 \\ 0 & \text{if } \mathcal{H}_1 \end{cases}, \quad (5)$$

where \mathcal{H}_0 and \mathcal{H}_1 represents the received signal $\mathbf{y}^{[j]}$ in the j -th time slot, originated from a legitimate IoT device and an illegitimate device, respectively, and act as the hypothesis for IoT device authentication. The conventional schemes [20], [33], [34] rely on quantization-based thresholds in (5) for decision making. However, the authentication performance significantly declines due to the quantization errors introduced by the algorithms. Additionally, it is challenging to obtain optimal values for the detection thresholds to maintain continuous authentication when a large number of IoT devices are involved since exhaustive search methods are utilized to obtain these values.

Another downside to these conventional schemes is that they rely on the physical channel for seed acquisition, verification, reconciliation, and IoT device authentication [5], [17], [18]. However, reliance on the physical channel for device authentication does not explicitly apply to resource-constrained IoT devices. The reasons for this are as follows.

- A transceiver pair cannot probe the physical channel simultaneously for seed acquisition due to the half-duplex nature of the radio. The resource-constrained IoT devices are assumed to probe the physical channel for seed acquisition and authentication in the conventional physical-channel-based schemes. This is impractical since the resource-constrained IoT devices cannot probe the physical channel due to their limited battery; therefore, the conventional schemes result in excessive battery loss and time lag due to the radio distance turnaround time.
- The reconciliation overhead due to imperfect physical-channel reciprocity increases with the increased key length for seed generation. This means that to achieve a higher authentication rate (by increasing key length), the parity bit information to correct errors is also increased. This is against the spirit of authentication mechanisms for resource-constrained IoT devices, where channel training/probing of IoT devices should be minimized due to their limited resources.
- A transceiver pair separated by a greater than half wavelength distance does not guarantee independent physical channels for seed acquisition [35]. This means that there is no clear safeguard distance to ensure the secrecy of the generated key, as typically assumed in the physical-channel-based seed acquisition techniques [36].

From this discussion, we can conclude that (i) conventional physical-channel-based authentication techniques exhibit these intrinsic limitations, which limits their effectiveness in situations where a transceiver pair experiences spoofing attacks, and (ii) the conventional physical-channel-based seed acquisition techniques are not practical for resource-constrained IoT devices. Therefore, access to a coherent source for identical and lightweight seed generation is crucial for continuous authentication between the AP and resource-constrained IoT devices.

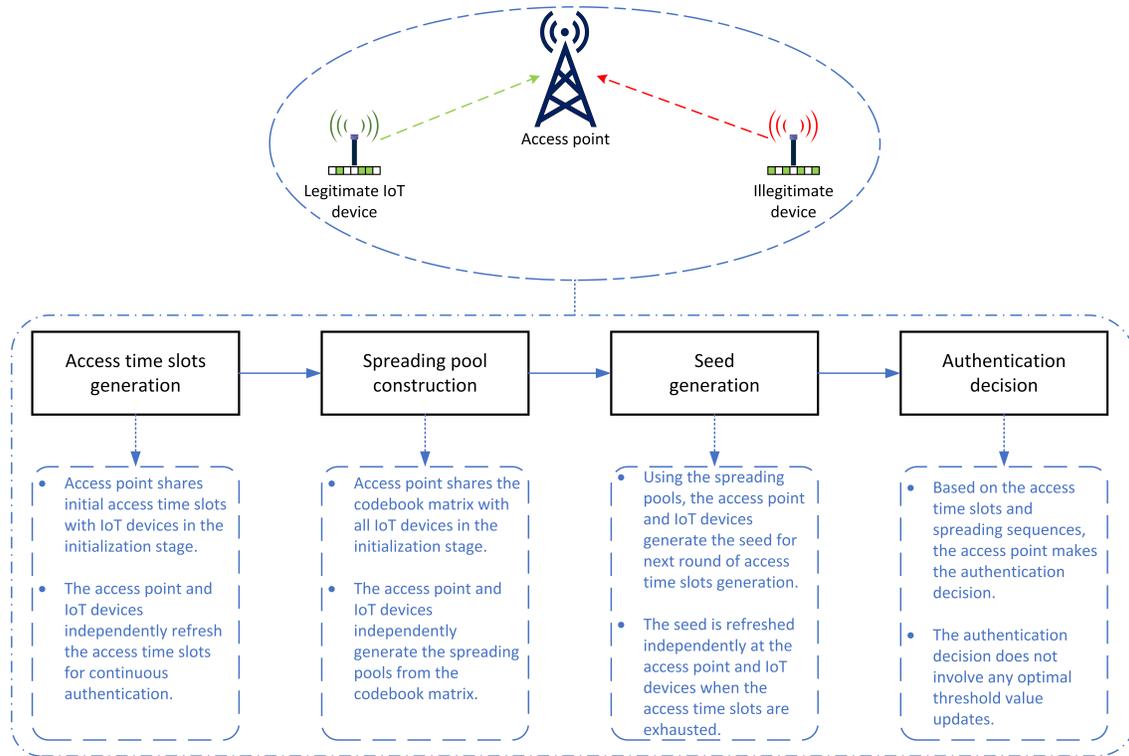


Fig. 2: Proposed authentication scheme comprises four processes: access time slots generation, spreading pool construction, seed generation, and authentication decision.

IV. PROPOSED AUTHENTICATION SCHEME

With the sporadic nature of transmission of IoT devices in mind, the objective at the AP is to authenticate the legitimate IoT devices from the received signal $\mathbf{y}^{[j]}$ in the j -th time slot. Therefore, to achieve authentication, the generated seeds must adhere to the policies as follows [15]: 1) a transceiver pair must generate an identical seed stemming from an identical feature for authentication at the AP; 2) seeds should be undisclosed to any other devices, making the generated feature unpredictable by illegitimate devices; and 3) seeds should be proactively refreshed to maintain continuous authentication while preserving uncertainty for illegitimate devices. To meet these requirements, we use the transmission nature of the grant-free NOMA in (4) as the seed source instead of relying on physical-channel attributes for seed acquisition. Then, we use the seed to generate the access time slots for IoT device authentication.

The proposed authentication scheme consists of four processes: (A) access time slots generation, (B) spreading pool construction, (C) seed generation, and (D) authentication decision, and is summarised in Fig. 2. The four processes form a cohesive, secure, continuous authentication system between an AP and IoT devices. The AP shares initial access time slots and a codebook matrix with the IoT devices in the initialization stage. The AP and IoT devices then independently refresh the access time slots and generate spreading pools from the codebook matrix. These spreading pools generate the seed for the next round of access time slots. When the current access time slots are exhausted, the seed is refreshed independently

at the AP and IoT devices. Finally, the AP uses the access time slots and spreading sequences to make authentication decisions without needing optimal threshold value updates. By combining these processes, the system ensures that the AP and IoT devices can securely communicate, authenticate each other, and maintain continuous authentication over time. This interaction of the proposed authentication scheme with the grant-free NOMA system is illustrated in Fig. 3. The four processes are further explained in detail below.

A. Access Time Slots Generation

The access time slots for IoT device transmission are divided into recurring time slots of fixed length [15], as depicted in Fig. 1. The IoT devices transmit their signals to the AP in time slots pre-agreed upon between the IoT devices and the AP. Therefore, the AP can quickly identify an illegitimate device based on its time slot access. If the seeds are hidden from illegitimate devices, the access time slots are highly unpredictable. More importantly, a seed can generate several access time slots, allowing each IoT device at the AP to be identified continuously for an extended period. Unlike conventional key-based physical-channel schemes, authentication via access time slots does not entail complex computation or high latencies because, in key-based schemes, access to a coherent key is required for every message transmission. In contrast, the access time slots do not require a shared key for every transmission since the transmission schedules are followed by the IoT device and verified by the AP. Thereby, continuous and lightweight authentication between a transceiver is achieved.

matrix to support $K = 6$ devices using $N = 4$ resource blocks in an overloaded³ scenario, given as

$$\mathbf{C}_{(4,6)} = \begin{bmatrix} w_0 & w_4 & w_3 & w_1 & w_6 & w_5 \\ 0 & w_2 & w_6 & w_4 & w_5 & w_0 \\ w_4 & w_7 & w_0 & w_3 & w_0 & 0 \\ w_3 & w_0 & w_2 & w_4 & w_3 & w_6 \end{bmatrix}, \quad (7)$$

where w_n is the non-zero elements of the codeword. The non-binary and complex-valued spreading sequences in (7) allow for a higher degree of freedom for loading a larger number of IoT devices, thus providing much more flexibility in spreading sequences design, which is reflected by a high overloading factor and demonstrates a true sense of grant-free transmission⁴.

Conventionally in grant-free systems, the codebook matrix in (3) is stored locally with the AP and shared with all IoT devices independently in the initialization stage, which is later utilized by the IoT devices for data transmission [2], [43]. With this sense of practicality in mind, we propose constructing a lightweight mechanism to utilize the codebook matrix in (3) for enhanced authentication. This involves constructing spreading pools from the codebook matrix in (3) for every IoT device in a cell. Let γ_k denote the spreading pool constructed using the codebook matrix $\mathbf{C}_{(4,6)}$ in (7) for the k -th IoT device. As such, for the overloaded scenario in (7), the respective spreading pools for $K = 6$ IoT devices can be constructed as

$$\begin{aligned} \gamma_1 &= \{w_0, 0, w_4, w_3\}, \\ \gamma_2 &= \{w_4, w_2, w_7, w_0\}, \\ \gamma_3 &= \{w_3, w_6, w_0, w_2\}, \\ \gamma_4 &= \{w_1, w_4, w_3, w_4\}, \\ \gamma_5 &= \{w_6, w_5, w_0, w_3\}, \\ \gamma_6 &= \{w_5, w_0, 0, w_6\}. \end{aligned} \quad (8)$$

Once the spreading pools are constructed, the access time slots are superimposed over the spreading pools for intelligent transmission and enhanced authentication. Thus, the spreading pools in (8) can therefore be rewritten as

$$\begin{aligned} \gamma_1 &= \left\{ \overbrace{w_0}^1, \overbrace{0}^1, \overbrace{w_4}^0, \overbrace{w_3}^0 \right\}, \\ \gamma_2 &= \left\{ \overbrace{w_4}^1, \overbrace{w_2}^1, \overbrace{w_7}^0, \overbrace{w_0}^1 \right\}, \\ \gamma_3 &= \left\{ \overbrace{w_3}^1, \overbrace{w_6}^0, \overbrace{w_0}^0, \overbrace{w_2}^0 \right\}, \\ \gamma_4 &= \left\{ \overbrace{w_1}^1, \overbrace{w_4}^1, \overbrace{w_3}^1, \overbrace{w_4}^0 \right\}, \\ \gamma_5 &= \left\{ \overbrace{w_6}^1, \overbrace{w_5}^0, \overbrace{w_0}^0, \overbrace{w_3}^0 \right\}, \\ \gamma_6 &= \left\{ \overbrace{w_5}^1, \overbrace{w_0}^1, \overbrace{0}^1, \overbrace{w_6}^0 \right\}. \end{aligned} \quad (9)$$

³The overloading factor is defined as the ratio of the number of potential IoT devices to the number of available resource blocks in the system, *i.e.*, overloading factor (%) = $\frac{K}{N} \times 100$.

⁴The design of the codebook matrix can be carried out in different ways [2], [40]–[42] to enhance the overloading factor of the system further. However, this is outside the scope of this work.

From (9), it can be seen that by jointly utilizing the spreading pools and access time slots, an enhanced security mechanism can be developed, which provides a higher degree of system efficiency (reduction in spreading sequence collision due to intelligent transmission) and security entropy (a two-step mechanism for device authentication). The utilized spreading pools by the respective IoT devices are then used for seed and refreshed access time slot generation. Herein, it should be noted that a longer length of spreading pool and access time slots results in a higher authentication entropy. However, a shorter length results in lower bit-error-rate (BER) performance. This demonstrates a trade-off between authentication and BER performance which can be controlled based on the network requirements.

C. Seed Generation

Once the spreading pools and their tagged access time slots are exhausted, the AP and IoT devices need to recreate newer spreading pools and access time slots for continuous authentication. In this regard, the k -th IoT device can use its current spreading pool to generate a seed value for the newer pools. Let $(c_{1k}, c_{2k}, \dots, c_{Nk})$ represent the length of the spreading sequences inside a spreading pool γ_k , and $(l_{1k}, l_{2k}, \dots, l_{Lk})$ represent the access time slots of the k -th IoT device. Then, we generate the seed by taking the XOR of the access time slots and calculating the ℓ_2 norm of the tagged spreading sequences. This process for an arbitrary spreading pool γ_k of the k -th IoT device is as follows:

Step 1: Take the original spreading pool and its superimposed access time slots

$$\gamma_k = \left\{ \overbrace{w_0}^1, \overbrace{0}^1, \overbrace{w_4}^0, \overbrace{w_3}^0 \right\} \quad (10)$$

Step 2: Take XOR of the access time slots

$$\gamma_k = \left\{ \overbrace{w_0}^0, \overbrace{0}^0, \overbrace{w_4}^1, \overbrace{w_3}^1 \right\} \quad (11)$$

Step 3: Nullify the spreading sequences under 0's

$$\gamma_k = \left\{ \overbrace{0}^0, \overbrace{0}^0, \overbrace{w_4}^1, \overbrace{w_3}^1 \right\} \quad (12)$$

Step 4: Take the sum and ℓ_2 norm of the spreading sequences under 1's to obtain preliminary seed

$$\Theta = \|w_4 + w_3\|_2 \quad (13)$$

Step 5: Take the square of the preliminary seed to obtain the final seed

$$seed = \Theta^2. \quad (14)$$

This process is performed independently at the AP and the IoT devices. It should be noted that steps 4 and 5 depend on the resource availability of the IoT devices. That is to say; if the IoT devices are extremely resource-constrained, the preliminary Θ can be used for access time slots generation since it averts computationally expensive $\mathcal{O}(L^2)$ operation in step 5, as well as results in a shorter key length. However, step 5 provides a longer key length for increased authentication, thereby providing prolonged authentication. The choice of seed in steps

4 and 5 demonstrates a trade-off between the computational performance and security performance of a transceiver pair. Hence, this process should be well-designed to achieve a better trade-off. Furthermore, it should be noted that, unlike the conventional physical-channel-based schemes, the proposed authentication scheme does not rely on channel probing for seed acquisition, seed reconciliation, or authentication. This means that the seed verification phase, which is required in the conventional physical-channel-based authentication schemes due to either imperfect channel probing or quantization errors, is not needed in the proposed authentication scheme, thus paving the way for a practical, lightweight, and independent authentication mechanism in a grant-free NOMA system.

D. Authentication Decision

The conventional physical-channel-based authentication schemes rely on quantization-aided hypothesis testing as a decision criterion in (5). However, such benchmarks rely on static statistical properties of the physical channel and cannot account for varying attributes of fast-fading physical-channel characteristics, resulting in misdetection. As opposed to this, the proposed authentication scheme does not rely on a quantization-based threshold as an authentication criterion. Instead, the proposed scheme utilizes a two-step authentication decision process, where the AP first matches the access time slots of the transceiver pair and then compares the spreading sequences of the following transmitting schedule. The two-step authentication process enables mitigating misdetection at the AP and averts false alarms. This authentication process is summarised in Algorithm 1, and the main procedure is presented as follows.

- 1) *Line 2*: The sparse transmitted signal vector in the j -th time slot is estimated and detected at the AP by the least squares algorithm as [44]:

$$\hat{\mathbf{x}}^{[j]} = \left(\mathbf{G}^{[j]}\right)^\dagger \mathbf{y}^{[j]}. \quad (15)$$

- 2) *Line 3*: The codebook matrix $\mathbf{C}^{[j]}$ utilized by the IoT devices in the j -th time slot is extracted by applying Hadamard division on the channel matrix as:

$$\mathbf{C}^{[j]} = \mathbf{G}^{[j]} \oslash \mathbf{H}^{[j]}. \quad (16)$$

- 3) *Line 6*: The spreading pools and the transmission schedule of the K IoT devices is extracted from the codebook matrix in the j -th time slot as:

$$\gamma_k^{[j](l)}[\text{device}] = \mathbf{C}^{[j]}(:, k). \quad (17)$$

- 4) *Line 7-12*: The l -th access time slot of the k -th IoT device $\gamma_k^{[j](l)}[\text{device}]$ in the j -th time slot is compared with the l -th access time slot of the AP $\gamma_k^{[j](l)}[\text{AP}]$ in the j -th time slot. If the access time slot matches, the authenticated devices indicator function $\Gamma_k^{[j]}$ for the k -th device in the j -th time slot is set to 1. Otherwise, the indicator function records a 0, deeming the k -th device as illegitimate.

- 5) *Line 13-17*: The l -th spreading sequence of the k -th IoT device $\gamma^{[j]}(k, l)[\text{device}]$ from the extracted spreading

Algorithm 1 The Proposed Authentication Scheme.

Input:

Received signals: $\mathbf{Y} = [\mathbf{y}^{[1]}, \mathbf{y}^{[2]}, \dots, \mathbf{y}^{[J]}]$;

Equivalent channel matrices: $\bar{\mathbf{G}} = [\mathbf{G}^{[1]}, \mathbf{G}^{[2]}, \dots, \mathbf{G}^{[J]}]$.

Output:

Authenticated devices indicator: $\bar{\Gamma} = [\Gamma^{[1]}, \Gamma^{[2]}, \dots, \Gamma^{[J]}]$;

Authenticated devices symbols: $\tilde{\mathbf{X}} = [\tilde{\mathbf{x}}^{[1]}, \tilde{\mathbf{x}}^{[2]}, \dots, \tilde{\mathbf{x}}^{[J]}]$.

Device detection

- 1: **for** $j = 1$ to J **do**
- 2: $\hat{\mathbf{x}}^{[j]} = \left(\mathbf{G}^{[j]}\right)^\dagger \mathbf{y}^{[j]}$
- 3: $\mathbf{C}^{[j]} = \mathbf{G}^{[j]} \oslash \mathbf{H}^{[j]}$

Device authentication

- 4: **for** $l = 1$ to L **do**
- 5: **for** $k = 1$ to K **do**
- 6: $\gamma_k^{[j](l)}[\text{device}] = \mathbf{C}^{[j]}(:, k)$.
- 7: *Step 1: (Access time slot check)*
- 8: **if** $\gamma_k^{[j](l)}[\text{AP}] == \gamma_k^{[j](l)}[\text{device}]$ **then**
- 9: $\Gamma_k^{[j](l)} = 1$.
- 10: **else**
- 11: $\Gamma_k^{[j](l)} = 0$.
- 12: Skip to line 17.
- 13: **end if**
- 14: *Step 2: (Spreading sequence check)*
- 15: **if** $\gamma^{[j]}(k, l)[\text{AP}] == \gamma^{[j]}(k, l)[\text{device}]$ **then**
- 16: $\Gamma_k^{[j](l)} = 1$.
- 17: **else**
- 18: $\Gamma_k^{[j](l)} = 0$.
- 19: **end if**
- 20: **end for**
- 21: **end for**
- 22: $\tilde{\mathbf{x}}^{[j]} = \hat{\mathbf{x}}^{[j]} \oslash \Gamma^{[j]}$.
- 23: **end for**

Return:

$\bar{\Gamma} = [\Gamma^{[1]}, \Gamma^{[2]}, \dots, \Gamma^{[J]}]$;

$\tilde{\mathbf{X}} = [\tilde{\mathbf{x}}^{[1]}, \tilde{\mathbf{x}}^{[2]}, \dots, \tilde{\mathbf{x}}^{[J]}]$.

pool in the j -th time slot is compared with the l -th spreading sequence of the AP $\gamma^{[j]}(k, l)[\text{AP}]$ in the j -th time slot. If the spreading sequence matches, the authenticated devices indicator function $\Gamma_k^{[j]}$ for the k -th device in the j -th time slot is set to 1. Otherwise, the indicator function records a 0, deeming the k -th device as illegitimate.

- 6) *Line 20*: The authenticated devices data $\tilde{\mathbf{x}}^{[j]}$ in the j -th time slot is determined by calculating the Hadamard product between the estimated sparse transmitted signal vector $\hat{\mathbf{x}}^{[j]}$ and the authenticated devices indicator function $\Gamma^{[j]}$ in the j -th time slot, given as:

$$\tilde{\mathbf{x}}^{[j]} = \hat{\mathbf{x}}^{[j]} \oslash \Gamma^{[j]}. \quad (18)$$

At the end of the iteration, the authenticated devices data $\tilde{\mathbf{x}}^{[j]}$ in the j -th time slot is transformed into a sparse vector, where the data of the illegitimate devices is replaced with 0's, whereas the authenticated devices data is recovered.

V. SECURITY PERFORMANCE ANALYSIS

The performance of any new authentication scheme can be assessed using security analysis. A comprehensive formal security analysis often necessitates sophisticated modelling, which entails using advanced mathematical frameworks and cryptographic primitives to replicate potential threat scenarios and evaluate system vulnerabilities. In such modelling, formal methods and symbolic representations are employed to capture and analyze the intricate dynamics of potential attacks and the protective countermeasures of the system. This intricate modelling process aims to uncover hidden vulnerabilities, test the system's resilience against various threats, and derive insights for strengthening the system's defence mechanisms [45]. However, a formal security analysis is outside the scope of this work. Instead, similar to [15], the effectiveness of our proposed authentication scheme can be assessed rigorously using performance metrics such as entropy, key space, and computational efficiency. Here is why these metrics are employed:

- **Entropy:** This metric indicates a system's resilience against unauthorized access. Specifically, greater entropy suggests that an illegitimate device would be computationally arduous to predict or deduce the system's state.
- **Key Space:** This metric represents the total set of potential keys that could be employed within the system, offering a quantifiable measure of its complexity against brute-force attacks.
- **Lightweight:** This metric aims to minimize computational demands and resource consumption while maintaining stringent security standards.

By focusing on these metrics, we can demonstrate the robustness and security performance of the proposed authentication scheme.

A. Entropy

Legitimate IoT devices go through periodic updates of the access time slots and spreading pools; therefore, it is challenging for illegitimate devices to spoof the AP. Furthermore, since a transceiver pair independently but identically utilizes multiple spreading sequences from the spreading pool for seed generation, they are difficult for illegitimate devices to predict. Following this, it is clear that the seed is concealed from an adversary if it does not know the access time slots and the corresponding spreading pools. Furthermore, updating the access time slots and spreading pools will provide further protection for legitimate IoT devices by renewing their access sequences over time. Hence, the proposed authentication scheme provides enhanced protection against spoofing attacks and pertains to legitimate communications between IoT devices and the AP.

With this understanding, entropy is defined as a metric that measures the uncertainty associated with the randomness of a system [46] and is used to evaluate the security strength of the authentication scheme. Thus, entropy is defined as

$$E_{total} = \sum_{r=1}^R E_r, \quad (19)$$

where

$$E_r = -p_{r0} \log p_{r0} - (1 - p_{r0}) \log(1 - p_{r0}). \quad (20)$$

R represents the total length of the shared key, and p_{r0} denotes the posterior probability of the r -th bit when it is 0 from the illegitimate devices' knowledge.

Lemma 1: The entropy of the proposed authentication scheme is higher than that of the physical-channel key generation schemes of [46]–[49].

Proof: We provide proof using heuristic arguments as follows. Assuming R denotes the length of the access time slots and the key in the physical-channel key generation schemes, we denote p_{r0}^I and p_{r0}^{II} as their posterior probabilities of the r -th bit when it is 0 from the illegitimate devices' knowledge, respectively. It should be noted that the proposed authentication scheme relies on multiple attributes, *i.e.*, it utilizes N spreading sequences for seed generation. On the contrary, the physical-channel key generation schemes rely on a single attribute for shared key generation. Since multiple attributes are being utilized in the proposed authentication scheme and legitimate IoT devices follow the pre-agreed access time slots for transmission, it is difficult for illegitimate devices to spoof the AP. Then,

$$\left| p_{r0}^I - \frac{1}{2} \right| < \left| p_{r0}^{II} - \frac{1}{2} \right| \quad (21)$$

holds [15], which means the illegitimate devices have less knowledge that the r -th bit is 0 in the proposed authentication scheme. Let E_r^I denote the entropy of the proposed authentication scheme, and E_r^{II} denote the entropy of the physical-channel key generation schemes. Then, from (21), we can concur that

$$E_r^I > E_r^{II} \quad (22)$$

holds. This completes the proof.

B. Key Space

Due to their limited computational resources, the resource-constrained IoT devices cannot compute shared keys for every data transmission, required by conventional encryption methods. To overcome this inherent issue, resource-constrained IoT devices rely on shortened keys to reduce the computational overhead. However, shortened keys can be more vulnerable to malicious attacks as they can be easily cracked by attackers using brute force. This is because sophisticated attackers with rapidly growing processing power can compromise the short-length keys within a much shorter time than before, for example, by using exhaustive search approaches [36]. Therefore, an additional layer of security based on low computational cost is required. Based on multi-factor attributes, the proposed authentication method complements the overall security paradigm by acting as another source of randomness to provide additional entropy to the system. This authentication at the lower layer compensates for entropy loss due to the use of shortened keys in the higher layers in resource-constrained IoT devices.

Lemma 2: The key space of the proposed authentication scheme is higher than that of the physical-channel key generation schemes of [46]–[49].

TABLE II: Key length versus search space complexity of physical-channel-based and proposed techniques.

Key length	Physical-channel key generation schemes		Proposed authentication scheme	
	Search space	Authentication complexity	Search space	Authentication complexity
9	512	$\mathcal{O}(\mathcal{N})$	8192	$\mathcal{O}(1)$
11	2048		32768	
13	8192		131072	
15	32768		524288	
17	131072		2097152	

Proof: We provide proof using heuristic arguments as follows. Assuming that R represents the length of the key in the proposed authentication scheme and physical-channel key generation schemes, we denote κ_R^I and κ_R^{II} as the upper bound of the key search space, respectively. We know that the proposed authentication scheme utilizes the access time slots and the complex spreading sequences for IoT device authentication. On the other hand, the physical-channel key generation schemes rely on the attribute of the physical channel for key generation. Thus, in Table II, we demonstrate the key search space versus the key length of the proposed authentication scheme and physical-channel key generation schemes. It is evident that the proposed authentication scheme achieves a higher search space than the physical-channel key generation schemes for the same key length. This is because the proposed technique utilizes complex spreading sequences and access time slots, which adds another source of randomness to the system for key generation. Therefore, the proposed authentication scheme is less susceptible to brute force attacks than the physical-channel key generation schemes for the same key length. Thus, from Table II, it is concurred that

$$\kappa_R^I > \kappa_R^{II} \quad (23)$$

holds. This completes the proof.

Since the proposed authentication scheme introduces more randomness into the network, the total system entropy E_{total} is higher than physical-channel key generation schemes. Hence, the proposed authentication scheme can be integrated into the network to provide additional entropy for improving the system's resistance to attacks.

C. Lightweight

The proposed authentication scheme utilizes the transmission parameters and access time slots for IoT device authentication. Conversely, the proposed authentication scheme does not rely on physical-channel probing for IoT device authentication. As a result, the seed verification phase is not required in our proposed authentication scheme. More importantly, the proposed schemes provide continuous authentication by checking the spreading sequences and access time slots of the IoT devices instead of generating and verifying shared keys repeatedly. As a result, as shown in Table II, compared to the physical-channel-based key generation schemes, the proposed authentication schemes achieve a lower authentication complexity for \mathcal{N} times of authentication, which validates the lightweight nature of the proposed authentication scheme.

TABLE III: Access time slots generation using seed.

State	Observations
Spreading pool utilized between a transceiver pair	$\gamma = \{-4 - 4i, -0 + 8i, 1 - 1i, \dots, -2 + 2i, 4\}$
Seed extracted by the AP	1111010000000
Seed extracted by the IoT	1111010000000
Access time slots at the AP and IoT	100001000000111011010010101010011 1100011100001001001111011101001110 111110001110010111100111110010011 110110011110010000001

VI. RESULTS AND DISCUSSION

In this section, we evaluate the performance of the proposed authentication scheme in solving the device authentication problem. We plot the performance of three physical-channel-based authentication benchmark solutions: using binary hypothesis testing (BHT) [21], using machine learning-based SVM [50], and using deep neural network-based (NN) detection [51]. For these three benchmark solutions, the core architectures are borrowed from the respective works but their input configurations have been adjusted to our system model for a fair comparison. For these benchmark solutions, the estimates of the received signal strength indicator (RSSI), the channel impulse response (CIR), and the channel frequency response (CFR) are used as attributes from the physical channel for authentication [5]. Specifically, due to the correlation of adjacent CIRs and CFRs on the same path, the temporal process of the i -th subpath at the j -th time slot is given as [5]

$$h_i(j) = \zeta h_i(j-1) + \sqrt{(1-\zeta^2)\sigma_i^2} u_i(j-1), \quad (24)$$

where $\zeta \in [0, 1]$ represents the physical-channel correlation of two successive subpaths and u_i is a driving noise which is modeled as a zero-mean complex Gaussian random variable with unit variance [21]. The path loss between the AP and the k -th IoT device is modeled as $128.1 + 37.6 \log_{10}(d_i)$, where d_i is the distance (in km) [32]. Additionally, for the benchmark schemes, the physical channels of the illegitimate devices are assumed to be independent of the legitimate IoT devices, meaning the illegitimate devices are assumed to be at a distance greater than half wavelength from the legitimate IoT devices.

Assuming initial authentication between a transceiver pair in the j -th time slot, their observation characteristics are shown in Table III. As detailed in section III-C, the AP and IoT device independently extract the seed by utilizing the spreading pool used for data transmission. Since the seed source is the spreading pool, extracted from the codebook matrix and available with the transceiver pair locally, there is no requirement for seed verification. Therefore, once the seed is acquired, the AP and IoT independently generate the access time slots required for transmission. In this work, we utilize the following monic polynomial for the access time slots generation

$$f(x) = 1 + x^1 + x^3. \quad (25)$$

A. Experimental Setup

In the simulations, unless otherwise stated, $K = 200$ potential devices simultaneously share $N = 100$ resources.

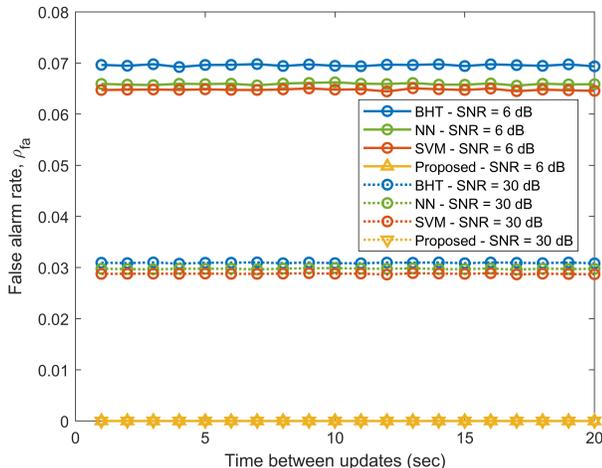


Fig. 4: False alarm rate, ρ_{fa} , versus the time between updates (sec), with the total number of potential devices $K = 200$, the number of resources $N = 100$, and the number of active devices $S = 20$.

Thus, the overloading factor (OF) is 200%. For every time slot, there is $S = 20$ number of active devices randomly selected from the set $\{1, 2, \dots, K\}$. The number of time slots is fixed at $J = 7$. The transmitted signals are modulated by Quadrature Phase Shift Keying. The signal-to-noise ratio (SNR) range is set between 0 to 25 dB. The oracle least squares algorithm is utilized for device detection.

The simulations are carried out on the Gadi supercomputer of the National Computational Infrastructure (NCI), Australia, utilizing 48 cores of Intel Xeon Platinum 8274 (Cascade Lake) processors and 192GB of random access memory. The simulations are carried out on MATLAB 2021b. The results are averaged over 1000 Monte Carlo trials.

B. Performance Metrics

In order to appropriately evaluate the authentication performance, we use the following metrics: the false alarm rate (ρ_{fa}), the misdetection rate (ρ_{md}), and the spreading sequence collision rate (ρ_{sc}) as performance metrics. Given the transmit signal \mathbf{x} , authenticated devices data $\tilde{\mathbf{x}}$, the authenticated devices indicator Γ , and the spreading pool γ for the k -th IoT device in the j -th time slot, the performance metrics are defined as follows.

- False alarm rate: This metric evaluates the rate of legitimate IoT devices being falsely detected as illegitimate devices, given as

$$\rho_{fa} = \frac{1}{K} \sum_{k \in \mathbf{x}^{[j]}} P \left\{ \Gamma_k^{[j]} = 0 \mid \mathbf{x}_k^{[j]} = 1 \right\}. \quad (26)$$

- Misdetection rate: This metric evaluates the rate of illegitimate IoT devices being misdetected, given as

$$\rho_{md} = \frac{1}{K} \sum_{k \in \mathbf{x}^{[j]}} P \left\{ \Gamma_k^{[j]} = 1 \mid \mathbf{x}_k^{[j]} = 0 \right\}. \quad (27)$$

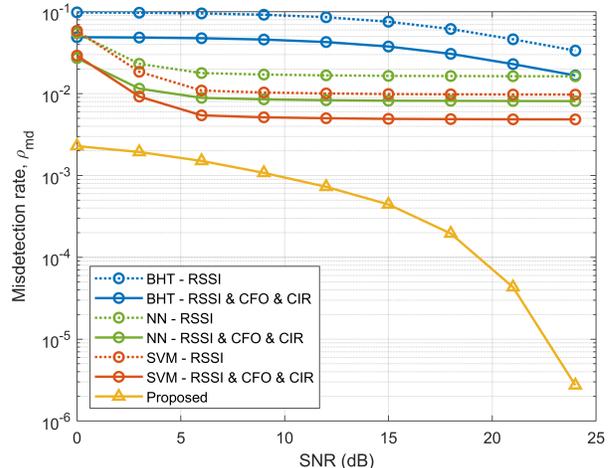


Fig. 5: Misdetection rate, ρ_{md} , versus SNR (dB), with the total number of potential devices $K = 200$, the number of resources $N = 100$, and the number of active devices $S = 20$.

- Spreading sequence collision rate: This metric evaluates the rate of legitimate IoT devices utilizing the same spreading sequence in the same access time slot, given as:

$$\rho_{sc} = \frac{1}{K} \sum_{k \in \tilde{\mathbf{x}}^{[j]}} P \left\{ \gamma_k^{[j](l)} == \gamma_{i \neq k}^{[j](l)} \right\}. \quad (28)$$

C. Authentication Performance

Fig. 4 plots the false alarm rate, ρ_{fa} , versus the time between updates (sec) for $K = 200$, $N = 100$, and $S = 20$. The false alarm events are avoided in the proposed authentication scheme due to the spreading sequences-based seed generation technique proposed in this paper. The spreading sequences-based seed generation allows AP and IoT devices to independently acquire identical seeds for the access time slots generation. In essence, the access time slots generated in the proposed authentication scheme between the AP and an IoT device are identical and do not require parity bits for seed reconciliation. On the contrary, since the benchmark schemes rely on estimates of multiple attributes of the physical channel, false alarm events are inevitable due to the imperfect and time-varying nature of the physical channel encountered due to reliance on the randomness of the channel for seed acquisition. Moreover, lower SNR could lead to a higher false alarm rate in physical-channel-based schemes since its performance explicitly relies on observing physical-channel attributes.

Fig. 5 plots the misdetection rate, ρ_{md} , versus SNR (dB) for $K = 200$, $N = 100$, and $S = 20$ ⁵. We can observe that in the entire SNR range, the proposed authentication scheme's misdetection rate decreases and achieves a near-threefold performance gain against the benchmark schemes at the higher SNR range. For instance, the performance gain is around 10 dB compared to the traditional BHT-based

⁵Fig. 5 is simulated with 100,000 Monte Carlo trials to evaluate its performance for the entire SNR range. This simulation took 19 hours to execute on the Gadi NCI supercomputer.

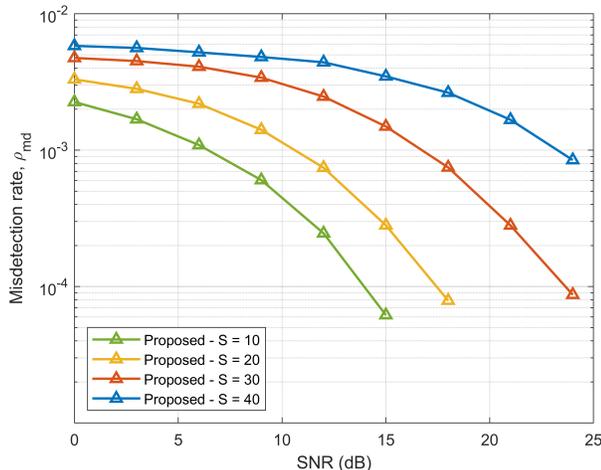


Fig. 6: Misdetection rate, ρ_{md} , versus SNR (dB) for the varying number of active devices S , with the total number of potential devices $K = 200$, and the number of resources $N = 100$.

authentication scheme at SNR = 6 dB. This trend is because the AP and IoT devices identically but independently generate the access time slots using the spreading sequences. These spreading sequences and the access time slots are then used for IoT device authentication. Hence, the proposed authentication scheme is robust in the noisy wireless communication environment. Fig. 5 also demonstrates the authentication performance of the benchmark schemes for single and multiple attributes, which rely on estimates of these attributes from the physical channel for device authentication. It can be seen that the benchmark schemes have a higher misdetection rate at lower SNR, which is due to the imperfect physical-channel mismatch between the AP and IoT devices, which requires the continuous updating of the decision boundary. More importantly, the reliance of the proposed authentication scheme on spreading sequences for continuous authentication adds an additional element to the authentication mechanism and generally makes it more difficult for an illegitimate device to spoof the AP under the proposed authentication protocol. By employing our proposed authentication scheme, the AP gains the ability to differentiate between legitimate and illegitimate devices based on their utilization of spreading sequences and transmission characteristics. Consequently, our proposed authentication scheme eliminates the disparities introduced by distance-related factors when distinguishing between legitimate and illegitimate devices, and therefore, the correlated physical channel characteristics do not play a role in spoofing the AP.

D. Robustness in Different Configurations

Fig. 6 plots the misdetection rate, ρ_{md} , versus SNR (dB) for the varying number of active devices S , with $K = 200$, and $N = 100$. It can be seen that the proposed authentication scheme is capable of handling a variety of active transmitting devices S . This is because the proposed authentication scheme

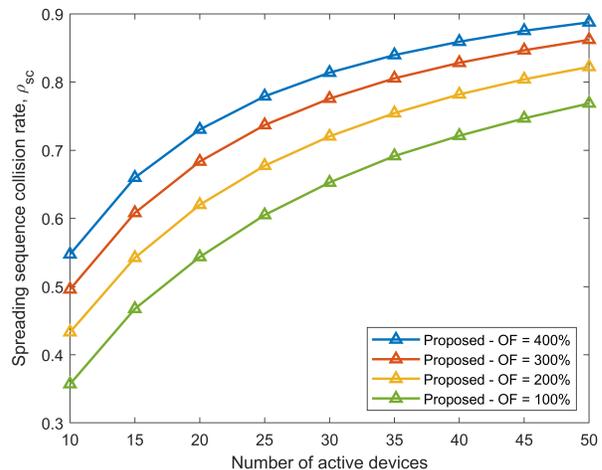


Fig. 7: Spreading sequence collision rate, ρ_{sc} , versus the varying number of active devices S , with the total number of potential devices $K = 200$.

does not rely on physical channels for binary testing as a decision boundary, which requires an update to the decision boundary for every change in the number of active devices S . Since the proposed authentication scheme relies on the spreading sequences extracted from the codebook matrix, the proposed authentication scheme can adapt to any number of active transmitting devices S . It should be noted that the reduction in misdetection rate ρ_{md} , caused by the increase in the number of active transmitting devices S is due to the device estimation errors, which is a side effect of the grant-free NOMA system.

Fig. 7 plots the spreading sequence collision rate, ρ_{sc} , versus the number of active devices S for different OF settings, with $K = 200$. The spreading sequence collision rate ρ_{sc} increases with the number of active devices S . It is also evident that a low number of resources N results in a higher OF, which also increases the spreading sequence collision rate ρ_{sc} . This is because when more active devices S transmit simultaneously with shared resources N , the probability of the two or more active devices using the same resource for transmission increases, which increases the spreading sequence collision rate ρ_{sc} . It should be noted that these collisions result from the system's bottleneck due to the inherent nature of the grant-free NOMA systems. Even so, the proposed authentication scheme can handle various active devices S and therefore is robust to different system settings.

Fig. 8 plots the misdetection rate, ρ_{md} , versus the time between updates (sec) for $K = 200$, $N = 100$, and $S = 20$. It can be seen that with the increase in the length L of the access time slots, the misdetection rate ρ_{md} of the proposed authentication scheme decreases. This is because the longer length of access time slots results in a more randomized transmission pattern for legitimate IoT devices, which is difficult for an illegitimate device to predict and spoof the AP. However, shorter lengths of access time slots, which result in a higher misdetection rate, are less computationally expensive

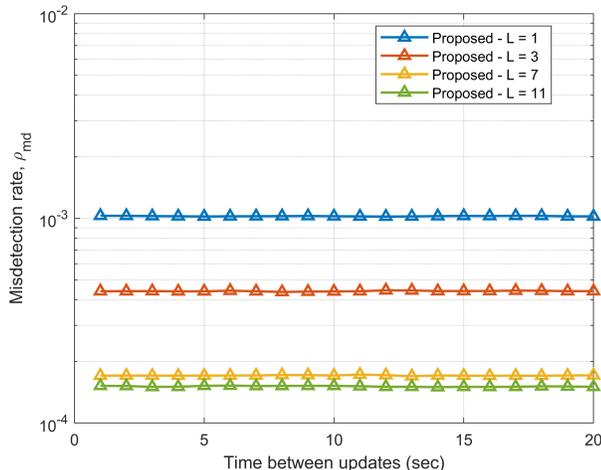


Fig. 8: Misdetection rate, ρ_{md} , versus the time between updates (sec) for the varying length of authentication sequence L , with the total number of potential devices $K = 200$, the number of resources $N = 100$, and the number of active devices $S = 20$.

to generate. Therefore, the choice between the length of the access time slots and the system's computational requirements is a trade-off that can be carefully chosen, depending on the requirement of the network.

Fig. 9 plots the computational cost versus the time between updates (sec) for $K = 200$, $N = 100$, and $S = 20$. It can be seen that the proposed authentication scheme attains a lower computational cost than the benchmark schemes. This is because the proposed authentication scheme relies on the access time slots and the spreading pools as its source of IoT device authentication. Since the codebook matrix, which is utilized to derive the spreading pools, is managed by the AP and does not require creating any threshold boundaries, the proposed scheme has a lower computational cost. On the contrary, the physical-channel-based benchmark schemes rely on a computationally expensive exhaustive search to derive decision boundaries for IoT device authentication. Furthermore, methods such as SVM and hypothesis testing are required for continuous parameter updates due to the time-varying nature of the physical channel for device authentication.

VII. CONCLUSION AND FUTURE WORK

In this paper, we proposed a secure and efficient continuous authentication scheme for IoT devices. Our scheme utilized the grant-free NOMA protocol's transmission characteristics as a source for seed generation and device authentication. By utilizing pre-arranged access time slots and spreading sequences of IoT devices at the AP, the proposed scheme eliminated the need for channel probing, seed reconciliation, and authentication. Simulation results demonstrated the effectiveness of the proposed scheme, with a near three-fold reduction in misdetection rate and close to zero false alarm rate in various system configurations. Additionally, our proposed scheme offered computational efficiency compared to benchmark schemes based on support vector machine and binary

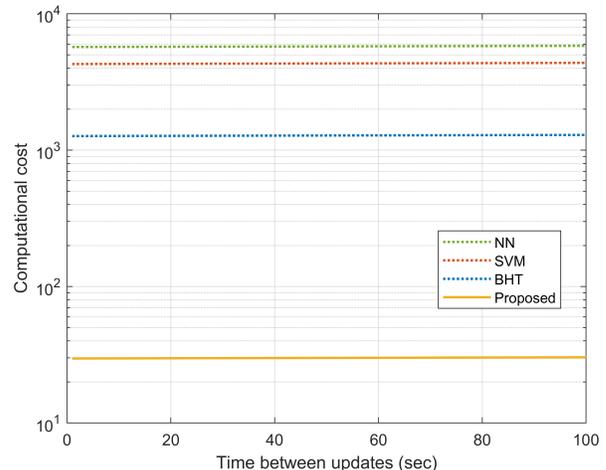


Fig. 9: Computational cost versus the time between updates (sec), with the total number of potential devices $K = 200$, the number of resources $N = 100$, and the number of active devices $S = 20$.

hypothesis testing utilizing physical channel information, with at least half the computational cost.

Future research should explore the extended application of the proposed authentication scheme beyond its current context in signature-based grant-free NOMA schemes, examining its adaptability in various scenarios to understand its effectiveness in diverse wireless communication environments. Additionally, investigating the authentication scheme's implementation in satellite-IoT networks presents an exciting opportunity to address unique challenges related to vast coverage and long-distance communication, potentially unlocking secure and efficient communication in satellite-based IoT applications. To ensure real-world viability, a comprehensive security analysis is crucial, covering a wide range of potential attacks, including adversarial and resource exhaustion attacks, to identify weaknesses and develop robust authentication solutions for IoT devices. Additionally, a formal security analysis of the authentication scheme can be carried out to further understand its workability in different scenarios. Furthermore, scalability should be investigated to ensure efficient authentication, even in massive-scale deployments. By optimizing the scheme without compromising security and addressing these research areas, the groundwork can be laid for secure, adaptive authentication solutions that bolster IoT device security and seamless integration into our interconnected world.

REFERENCES

- [1] S. Khan, C. Thapa, S. Durrani, and S. Camtepe, "Beyond key-based authentication: A novel continuous authentication paradigm for IoTs," in *Proc. IEEE GLOBECOM Wkshps*, Dec. 2023.
- [2] M. B. Shahab, R. Abbas, M. Shirvanimoghaddam, and S. J. Johnson, "Grant-free non-orthogonal multiple access for IoT: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1805–1838, May 2020.
- [3] "State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally," May 2022. [Online]. Available: <https://iot-analytics.com/number-connected-iot-devices/>

- [4] D. Nguyen, M. Ding, P. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. Poor, "6G internet of things: A comprehensive survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, Jan. 2022.
- [5] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 282–310, Dec. 2021.
- [6] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.
- [7] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Computing.*, vol. 9, no. 1, pp. 17–30, Jan. 2009.
- [8] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, Jun. 2016.
- [9] S. Khan, S. Durrani, M. B. Shahab, S. J. Johnson, and S. Camtepe, "Joint user and data detection in grant-free NOMA with attention-based BiLSTM network," *IEEE Open J. Commun. Soc.*, pp. 1–1, Jul. 2023.
- [10] I. Stelliou, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, Jul. 2018.
- [11] M. binti Mohamad Noor and W. H. Hassan, "Current research on internet of things (IoT) security: A survey," *Computer networks*, vol. 148, pp. 283–294, Jan. 2019.
- [12] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Mar. 2017.
- [13] H. Sharma, N. Kumar, B. K. Panigrahi, and A. Alotaibi, "Deep learning-based authentication framework for secure terrestrial communications in next generation heterogeneous networks," *IEEE Internet Things Mag.*, vol. 5, no. 4, pp. 174–179, Dec. 2022.
- [14] M. Abdrabou and T. A. Gulliver, "Adaptive physical layer authentication using machine learning with antenna diversity," *IEEE Trans. Commun.*, vol. 70, no. 10, pp. 6604–6614, Oct. 2022.
- [15] H. Fang, X. Wang, N. Zhao, and N. Al-Dhahir, "Lightweight continuous authentication via intelligently arranged pseudo-random access in 5G-and-beyond," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4011–4023, Mar. 2021.
- [16] R. H. Weber, "Internet of things—new security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, Jan. 2010.
- [17] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.
- [18] L. Y. Paul, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 1, pp. 38–51, Feb. 2008.
- [19] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, May 2014.
- [20] P. Zhang, Y. Shen, X. Jiang, and B. Wu, "Physical layer authentication jointly utilizing channel and phase noise in MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2446–2458, Jan. 2020.
- [21] N. Xie, J. Chen, and L. Huang, "Physical-layer authentication using multiple channel-based features," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2356–2366, Jan. 2021.
- [22] Y. Chen, P.-H. Ho, H. Wen, S. Y. Chang, and S. Real, "On physical-layer authentication via online transfer learning," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1374–1385, Jan. 2022.
- [23] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, Nov. 2019.
- [24] T. Qiu, Y. Zhang, D. Qiao, X. Zhang, M. L. Wymore, and A. K. Sangaiah, "A robust time synchronization scheme for industrial internet of things," *IEEE Trans. Industr. Inform.*, vol. 14, no. 8, pp. 3570–3580, Aug. 2018.
- [25] A. Elsts, X. Fafoutis, S. Duquenois, G. Oikonomou, R. Piechocki, and I. Craddock, "Temperature-resilient time synchronization for the internet of things," *IEEE Trans. Industr. Inform.*, vol. 14, no. 5, pp. 2241–2250, May. 2018.
- [26] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.
- [27] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf.*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.
- [28] J. B. Perazzone, L. Y. Paul, B. M. Sadler, and R. S. Blum, "Cryptographic side-channel signaling and authentication via fingerprint embedding," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 9, pp. 2216–2225, Sep. 2018.
- [29] B. Wang, L. Dai, T. Mir, and Z. Wang, "Joint user activity and data detection based on structured compressive sensing for NOMA," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1473–1476, Apr. 2016.
- [30] W. Kim, Y. Ahn, and B. Shim, "Deep neural network-based active user detection for grant-free NOMA systems," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2143–2155, Apr. 2020.
- [31] Y. Zou, Z. Qin, and Y. Liu, "Joint user activity and data detection in grant-free NOMA using generative neural networks," in *Proc. IEEE ICC.*, Aug. 2021, pp. 1–6.
- [32] "Evolved universal terrestrial radio access (E-UTRA); physical channels and modulation," in *3GPP Technical Report 36.211, v16.6.0*, Jun. 2021.
- [33] F. J. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE ICC*, Jun. 2013, pp. 4724–4728.
- [34] 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, Feb. 2016.
- [35] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proc. 4th Euro. Wksp. System Security*, Apr. 2011, pp. 1–6.
- [36] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.
- [37] P. H. Bardell, W. H. McAnney, and J. Savir, *Built-in test for VLSI: pseudorandom techniques*. Wiley-Interscience, 1987.
- [38] J. B. Fraleigh, *A first course in abstract algebra*. Pearson Education India, Dec. 2003.
- [39] Z. Yuan, G. Yu, W. Li, Y. Yuan, X. Wang, and J. Xu, "Multi-user shared access for internet of things," in *Proc. IEEE VTC-Spring*, Jul. 2016, pp. 1–5.
- [40] M. Taherzadeh, H. Nikopour, A. Bayesteh, and H. Baligh, "SCMA codebook design," in *Proc. IEEE VTC-Fall*, Sep. 2014, pp. 1–5.
- [41] B. Wang, K. Wang, Z. Lu, T. Xie, and J. Quan, "Comparison study of non-orthogonal multiple access schemes for 5G," in *Proc. IEEE BMSB*, Jun. 2015, pp. 1–5.
- [42] A. Alnoman, S. Erkucuk, and A. Anpalagan, "Sparse code multiple access-based edge computing for IoT systems," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 7152–7161, May 2019.
- [43] L. Liu, E. G. Larsson, W. Yu, P. Popovski, C. Stefanovic, and E. De Carvalho, "Sparse signal processing for grant-free massive connectivity: A future paradigm for random access protocols in the internet of things," *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 88–99, Sep. 2018.
- [44] B. Wang, L. Dai, Y. Zhang, T. Mir, and J. Li, "Dynamic compressive sensing-based multi-user detection for uplink grant-free NOMA," *IEEE Commun. Lett.*, vol. 20, no. 11, pp. 2320–2323, Aug. 2016.
- [45] I. Altaf, M. A. Saleem, K. Mahmood, S. Kumari, P. Chaudhary, and C.-M. Chen, "A lightweight key agreement and authentication scheme for satellite-communication systems," *IEEE Access*, vol. 8, pp. 46278–46287, Mar. 2020.
- [46] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Netw.*, vol. 21, no. 6, pp. 1835–1846, Aug. 2015.
- [47] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1779–1790, Sep. 2013.
- [48] M. Edman, A. Kiayias, Q. Tang, and B. Yener, "On the security of key extraction from measuring physical quantities," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 8, pp. 1796–1806, Aug. 2016.
- [49] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual ofdm subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, Jun. 2016.
- [50] T. M. Hoang, T. Q. Duong, H. D. Tuan, S. Lambotharan, and L. Hanzo, "Physical layer security: Detection of active eavesdropping attacks by support vector machines," *IEEE Access*, vol. 9, pp. 31595–31607, Feb. 2021.
- [51] R.-F. Liao, H. Wen, S. Chen, F. Xie, F. Pan, J. Tang, and H. Song, "Multiuser physical layer authentication in internet of things with data augmentation," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2077–2088, Mar. 2020.