IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 21, 2020, accepted October 13, 2020, date of publication October 26, 2020,
date of current version November 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3033562

A Novel Cross-Layer Authentication Protocol for the Internet of Things

YONGGU LEE[1], JISEOK YOON[2], (Graduate Student Member, IEEE), JINHO CHOI[3], (Senior Member, IEEE), AND EUISEOK HWANG[4], (Member, IEEE)

[1]Security Research and Devotement Team, Korea Atomic Energy Research Institute, Daejeon 34057, South Korea
[2]School of Mechatronics, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea
[3]School of Information Technology, Deakin University, Geelong, VIC 3220, Australia
[4]School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea

Corresponding author: Euiseok Hwang (euiseokh@gist.ac.kr)

This work was supported in part by the Institute for Information and Communications Technology Promotion (IITP) Grant Funded by the Korea Government (MSIT) under Grant 2017-0-00413, in part by the Streamlined Secure Communications by the Physical Layer Identification in Cellular IoT, and in part by the GIST Research Institute (GRI) Grant Funded by the GIST in 2020.

ABSTRACT An innovative cross-layer authentication protocol that integrates cryptography-based authentication and physical layer authentication (PLA) is proposed for massive cellular Internet of things (IoT) systems. Due to dramatic increases in the number of cellular IoT devices, a centralized authentication architecture in which a mobility management entity in core networks administers authentication of massive numbers of IoT devices may cause network congestion with large signaling overhead. Thus, a distributed authentication architecture in which a base station in radio access networks authenticates IoT devices locally is presented. In addition, a cross-layer authentication protocol is designed with a novel integration strategy under the distributed authentication architecture, where PLA, which employs physical features for authentication, is used as preemptive authentication in the proposed protocol. Theoretical analysis and numerical simulations were performed to analyze the trade-off between authentication performance and overhead in the proposed authentication method compared with existing authentication protocols. The results demonstrate that the proposed protocol outperforms conventional authentication and key agreement protocols in terms of overhead and computational complexity while guaranteeing low authentication error probability.

INDEX TERMS Authentication and key agreement, internet of things, physical layer authentication.

I. INTRODUCTION

With massive communication capacity and connectivity, the fifth-generation (5G) mobile network technology is considered the key enabler of the fourth industrial revolution [1]. However, despite the remarkable advances, security remains a serious problem [2], [3]. In particular, it has various security vulnerabilities, for example, due to the potential massive scale of connectivity and, limited hardware resources of IoT devices. Furthermore, as cyber physical critical infrastructure systems, e.g., smart grids have been deployed using 5G technology, ensuring security has become increasingly important. In particular, spoofing attacks whereby untrusted users with malicious intent attempt to masquerade as trusted users are a major concern in cyber physical systems (CPSs) because such attacks can result in economic loss and cause the physical infrastructure to become unstable.

Cryptographic authentication mechanisms have been studied and used to prevent spoofing attacks in cellular networks [4]–[15]. Instead of requiring a user password in human-type communications (HTC), it is possible to confirm the identity of a device for machine-type communications (MTC) by using cryptography-based authentication algorithms. An authentication and key agreement (AKA) protocol, which was standardized by the third generation partnership project (3GPP) has been used in wireless networks. The AKA protocol involves a challenge-response based authentication mechanism that uses symmetric cryptography and has been revised from the second-generation AKA protocol. Particularly, an evolved packet system AKA (EPS-AKA) protocol has been widely used for mutual authentication between a cellular network and a mobile device in long-term

The associate editor coordinating the review of this manuscript and approving it for publication was Chin-Feng Lai.

evolution (LTE) systems [16]. However, the EPS-AKA protocol suffers from traditional vulnerabilities (e.g., disclosure of user identity) and attacks such as denial-of-service (DoS) and replay attacks [17]. In addition, if a large number of IoT devices attempt to access a network in a short period, high network access latency and authentication signaling congestion will occur. Therefore, it is necessary to develop lightweight authentication protocols for the congestion avoidance in massive IoT systems.

Lightweight authentication protocols for massive IoT systems have been studied in [7]–[15], [18], [19]. In particular, several research works focus on group-based authentication for efficient authentication in massive networks [9]–[15]. In [9], a secure and efficient group AKA protocol named SE-AKA is presented to offer not only efficient group authentication but also a privacy enhancement of the international mobile subscriber identity (IMSI) by using a public key infrastructure (PKI). However, when a lot of MTC devices are attached, this initial message can possibly congest the network because the signaling between the mobility management entity (MME) and the home subscriber server (HSS) still contains information for every MTC devices in a group. In [10], a group-based AKA (G-AKA) scheme has been proposed to trust a group of IoT devices simultaneously and generate a session key with each IoT device by adopting the bilinear pairing technique and an aggregate signature scheme in LTE networks. However, the G-AKA scheme has high computational complexity which is impractical for low-cost IoT devices. In [12], the elliptic curve Diffie–Hellman (ECDH) protocol is used as a G-AKA protocol to protect the session key and realize group authentication with strong security.

Alternatively, physical layer authentication (PLA), which enables fast and lightweight authentication by exploiting physical characteristics (e.g., channel, and carrier frequency offset (CFO)) for authentication, has attracted attention as an authentication solution for IoT devices due to its efficiency and effectiveness [20], [21]. PLA can be divided into two cases, i.e., PLA without a shared PHY secret key and PLA with a shared PHY secret key, according to the purpose of the exploited physical layer (PHY) features. In PLA without a shared PHY secret key, PHY features are used directly as a secret key for authentication, whereas, in PLA with a secret key, they are employed for the encryption of a secret key shared between a pair of legitimate transceivers for authentication. In PLA without a shared PHY secret key, most PLA schemes make the best use of channel state information (CSI) for authentication [22]–[25]. In the time division duplex (TDD) mode, a channel can be easily shared between legitimate transceivers due to channel reciprocity. Except for that, other PHY features (e.g., CFO and hardware imperfections) are used as a secret key for authentication in [26]–[28]. These PLA schemes without a shared PHY secret key do not require an additional secret key (i.e., key management is not required). However, authentication performance of the PLA can be directly related to characteristics of PHY features because they play a role as a secret key. For example, if a malicious IoT device is located near a legitimate IoT device, a channel based PLA scheme cannot effectively defend impersonation attacks of the malicious IoT device because the channels depend on the transceiver's location.

PLA methods with a secret key have been studied previously [29]–[32]. In such methods, PHY features are employed to encrypt the secret key. While the PLA methods require a shared PHY secret key, its authentication performance is less sensitive to PHY features compared to PLA without a shared PHY secret key. In [29], a unified approach to compression and authentication of a signal is proposed to reduce computational complexity using a measurement matrix as a secret key in compressive sensing (CS). In addition, PHY challenge-response authentication mechanism (PHY-CRAM) schemes have been studied extensively in [30]–[32]. In these methods [31], [32], a channel phase sensitive to the locations of wireless transceivers is employed to encrypt a secret key in the challenge-response stages. However, if PHY features, which cannot be controlled, change rapidly, authentication performance can be degraded. For example, if coherence time is less than the authentication period, PHY-CRAM using CSI may reject a legitimate response signal due to the changed CSI. To avoid such authentication failures with the PHY only features, cross-layer authentication schemes that integrate PLA and cryptography-based authentication techniques have been proposed in [33]–[38]. In [36], hardware experiment for cross-layer authentication is performed to demonstrate advantages of combining PLA and cryptography-based authentication by using OpenAirInterface. In addition, a novel cross-layer authentication scheme is presented to ensure authentication performance stability under dynamic communication scenarios in [37]. However, authentication protocols that simply cascade both layer schemes might be inefficient in terms of signaling overhead and have limited practical applications.

In this article, we propose a cross-layer authentication protocol that applies PLA to an EPS-AKA protocol in massive IoT systems. To reduce overhead and delay caused by authentication of massive IoT devices, a distributed authentication architecture in which a base station (BS) authenticates of IoT devices in radio access networks (RANs) rather than using a MME in core networks is employed in this proposed protocol. In addition, PLA is used for distributed authentication in the proposed protocol. However, the authentication performance of PLA may be unsatisfactory in poor communication environments (e.g., low signal-to-noise ratio (SNR)); on the other hand, PLA schemes can provide small signaling overhead and short delay time for authentication. The proposed protocol can alleviate the authentication performance degradation of PLA and reduce signaling overhead of cryptography-based authentication by exploiting advantages of both PLA and cryptography-based authentication using a novel integration strategy. Through theoretical analysis and numerical simulation, we demonstrate that an authentication error probability can be set by determining two thresholds in

the proposed protocol. In addition, the proposed protocol has small signaling overhead and small computational complexity compared to conventional AKA protocols.

The main contributions of this article are summarized as follows:

- A cross-layer authentication protocol that integrates PLA and a conventional AKA is proposed for massive cellular IoT systems. The proposed protocol uses a novel integration strategy based on the test statistic result of PLA which is our previous work in [39]. In addition, it is a generalized version of a cross-layer authentication protocol in [39], where any PLA scheme can be applied to the proposed protocol.
- To reduce signaling overhead in cellular networks, a distributed authentication architecture is presented for massive IoT devices in this article. In addition, we simply categorize cellular IoT devices as follows: Class I, II and III (please refer to Section II). The proposed protocol targets authentication of Class III devices under the distributed authentication architecture.
- For sophisticated cross-layer authentication, we propose a novel integration strategy based on the test statistic result of PLA. By using this integration strategy, a proposed protocol can reduce the signaling overhead while providing a competitive authentication performance.
- Through theoretical analysis and numerical simulation, we analyze security, overhead, and complexity of the proposed protocol. In case of overhead, signaling and communication overheads of the proposed protocol are derived. In addition, we show a trade-off relationship between authentication performance and overhead in the proposed protocol.

The remainder of this article is organized as follows. Section II presents the motivation of this work. The proposed cross-layer authentication protocol is described in Section III. In Section IV, we analyze the proposed protocol in terms of security, overhead and complexity. The simulation results to evaluate the performance of the proposed protocol are presented in Section V. Finally, concluding remarks are given in Section VI.

Notation: Upper-case and lower-case boldface letters are used for matrices and vectors, respectively. $\mathcal{CN}(\mu, \sigma^2)$ represents the distribution of circularly symmetric complex Gaussian random variable with mean μ and variance σ^2.

II. MOTIVATION

5G is expected to enable ubiquitous connectivity, where massive devices to connected the network are used to realize CPSs (i.e., the IoT). However, 5G technology involves several security vulnerabilities that must be considered e.g., massive IoT devices, CPSs, and limited hardware capabilities. In particular, it is prone to active attacks (e.g., DoS, impersonation, man-in-the-middle attacks) due to the vulnerabilities. For example, assume that the numbers of mobile and MTC devices are 636, 000 and 6, 360, 000, respectively in 3GPP scenario [40]. Then, if conventional EPS-AKA is used for authentication in the scenario, the total signaling overhead for all devices becomes about 1.6×10^{11} bits. The heavy signaling burden implies a significant increase of the processing load on the control plane entities of the network (e.g., MME) and finally causes network congestion.

Heterogeneity of 5G that various kinds of devices attempt to communicate with each other in 5G networks should be considered for the design of an authentication protocol. For example, some IoT devices, e.g., smart meters send very short data packets in the networks. Then, conventional authentication mechanisms are inefficient for the IoT devices in terms of overhead, although they are suitable for authentication of devices that transmit streaming data (e.g., smartphone and tablet). Thus, different authentication protocols should be applied for each device type. In this article, we categorize such devices as follows: Class I is for HTC devices such as a mobilephone and Class II represents IoT devices with sufficient hardware capabilities (e.g., industrial IoT device, data concentrator unit). Class III represents massive IoT devices with limited hardware capabilities (e.g., smart meter and street lighting). Based on the device categorization, while conventional centralized security architectures in which entities (e.g., MME and HSS) in core networks charge all security in a centralized manner is appropriate for Class I and II devices, it is not suitable for Class III devices due to signaling inefficiency and limited hardware capabilities. It means that the Class III devices need a new security architecture to increase overhead efficiency and reduce computational complexity. So, it is important to develop a streamlined authentication protocol for massive IoT systems.

Motivated by the problems, a new security framework that imposes a burden of security (i.e., authentication) on RANs in a distributed manner is presented in this article (referred to as local security). As shown in Fig.1, a BS in RANs independently authenticates Class III devices to reduce excessive network traffic to the MME in the distributed authentication architecture. Based on the notion of local security, cross-layer authentication, which combines PLA with cryptography-based authentication, is employed as a solution for Class III device authentication in this article. This can reduce signaling overhead in core networks and the computational complexity of low-cost IoT devices using a PLA scheme in a cryptographic authentication mechanism. Physical characteristics (e.g., channel, and CFO) can substitute for the cryptographic algorithms (e.g., hash functions) in PLA. As a result, authentication can be made more secure in terms of information-theoretical security, while conventional cryptography-based authentication aims for computational security, which can be broken given sufficient computational capacity. Despite the advantages of PLA, PLA may not guarantee robust authentication reliability due to feature variation and environmental factors such as noise. In particular, it is frequent to authentication of Class III devices because Class III devices have limited power capabilities (i.e., low SNR). Therefore, a cross-layer authentication can be considered as a solution by taking both advantages of PLA

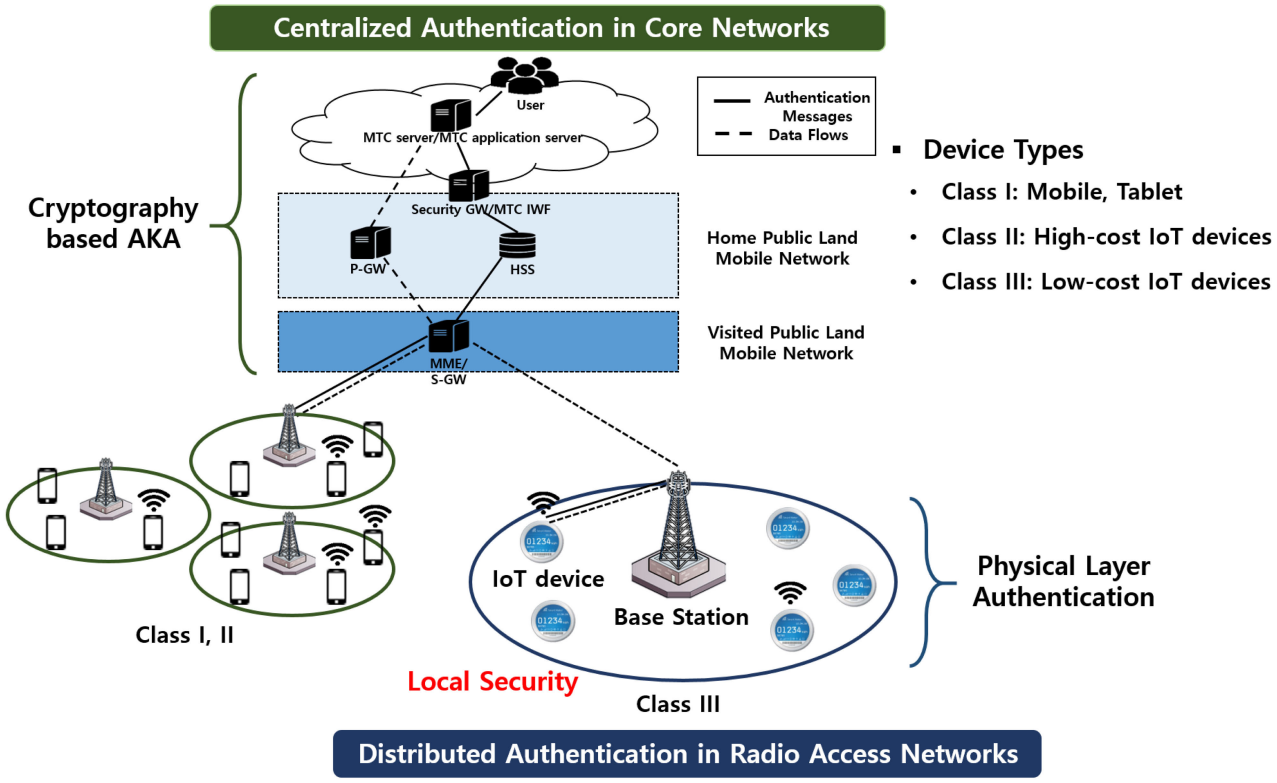


FIGURE 1. Proposed authentication architecture based on local security in cellular networks.

and cryptography-based authentication. However, its design has not been studied actively due to the independence of PLA and cryptographic authentication. In particular, existing cross-layer authentication schemes [33]–[35] do not consider both signaling overhead and authentication performance and there is no deep analysis for the performances of the cross-layer authentication scheme. In [33], a cross-layer authentication scheme is proposed to reduce delay in smart meter systems, but it cannot provide authentication reliability comparable to a cryptography-based authentication. On the other hand, cross-layer authentication protocols in [34], [35] cannot reduce overhead and delay, while it can enhance authentication performance by cascading PLA and cryptography-based authentication. Consequently, it is necessary to design a new cross-layer protocol that applies PLA to the cryptography-based authentication to reduce network traffic in massive IoT while guaranteeing reasonable authentication performance.

III. PROPOSED CROSS-LAYER AUTHENTICATION PROTOCOL

In this section, we present the proposed cross-layer authentication protocol, which integrates PLA and cryptography-based authentication (i.e., AKA) for massive IoT systems.

A. INTEGRATION STRATEGY FOR CROSS-LAYER AUTHENTICATION

In this subsection, we briefly introduce our previously proposed integration strategy [39], which is implemented in the proposed cross-layer authentication approach. The integration problem is a key issue in cross-layer authentication because it can significantly affect authentication performance and signaling overhead. We aim to design cross-layer authentication for low-cost IoT devices to reduce signaling overhead, and maintain reasonable authentication performance under bad communication environments.

PLA enables fast and lightweight authentication with small signaling overhead; however, PLA demonstrates lower authentication performance than cryptography-based authentication techniques. Thus, in the integration strategy [39], a PLA scheme is employed as preemptive authentication between an IoT device and the BS. After performing the PLA, the need to perform cryptography-based authentication in the proposed protocol is determined according to the preemptive authentication result. Generally, the PLA result is based on a test statistic, which is influenced by the communication environment, e.g., channel and noise. Thus, it can cause an error in authentication (i.e., binary hypothesis testing) at a low probability in PLA. Therefore, it is important to define a vague result of the test statistic.

As a result, the preemptive authentication result in the proposed protocol is divided into three cases: 'Rejected', 'Ambiguous' and 'Authenticated', while conventional PLA only determines whether a received signal is legitimate or an intrusion signal. In 'Rejected' and 'Authenticated', the BS can be sure about whether the received signal is from an intruder or a legitimate IoT device, respectively, with a

high probability. On the other hand, in 'Ambiguous', the BS is not sure about whether or not the signal is legitimate. That is, we stipulate that 'Ambiguous' is an ambiguous result that is difficult to determine whether it is 'Rejected' or 'Authenticated' in the physical layer, which is processed by the upper layer cryptography-based authentication. This is a key point in the integration strategy. Then, to determine a preemptive result among the three cases (i.e., 'Rejected', 'Ambiguous' and 'Authenticated') in PLA, two thresholds denoted α_0 and α_1 are used in PLA, while a conventional PLA method employs a threshold to differentiate 'Rejected' and 'Authenticated' cases. Here, for given target miss and false alarm probabilities (denoted P_M° and P_F°, respectively), the thresholds are determined as follows:

$$\alpha_1 = \arg\max_{\alpha} F_{\eta|\mathcal{H}_1}(\alpha) \leq P_M^\circ, \tag{1}$$

and

$$\alpha_0 = \arg\max_{\alpha} (1 - F_{\eta|\mathcal{H}_0}(\alpha)) \leq P_F^\circ, \tag{2}$$

where $F_{\eta|\mathcal{H}_i}(x)$ is the cumulative distribution function of $\eta|\mathcal{H}_i$ for $i = 0, 1$. Here, η is a test statistic for authentication decision and $\mathcal{H}_1$ and $\mathcal{H}_0$ are the alternative hypothesis, i.e., the received signal is transmitted by a legitimate IoT device and the null hypothesis, i.e., the received signal is transmitted by an intrusion device, respectively.

For easy comprehension, suppose a channel based PLA using a test statistic of $\eta = \text{corr}(\mathbf{H}_A, \mathbf{H}_U)$ for an authentication decision, where $\mathbf{H}_A$ and $\mathbf{H}_U$ denote the stored channel matrix used as a secret key and the estimated channel matrix from a received signal, respectively. In addition, corr($\mathbf{x}$, $\mathbf{y}$) is the correlation coefficient between $\mathbf{x}$ and $\mathbf{y}$. Then, as shown in Fig.2, although distributions of η for legitimate and intrusion signals are different, they can be slightly close due to bad communication environment (e.g., SNR), and it results a poor authentication performance. So, as mentioned earlier, in the proposed integration strategy, areas for the three cases are determined with α_0 and α_1 as follows:

$$\Theta = \begin{cases} \text{Rejected} & \text{if } \eta \leq \alpha_1 \\ \text{Ambiguous} & \text{if } \alpha_1 \leq \eta \leq \alpha_0 \\ \text{Authenticated} & \text{if } \eta \geq \alpha_0. \end{cases} \tag{3}$$

Thus, if the preemptive result is 'Authenticated' or 'Rejected', authentication is complete (i.e., cryptography-based authentication is not performed). On the other hand, if the result is 'Ambiguous', cryptography-based authentication is performed to make a final authentication decision at the MME.

B. PROPOSED PROTOCOL

In this subsection, we propose a cross-layer authentication protocol that prevents severe network congestion in core networks and minimize the computational complexity for authentication for low-cost IoT devices in massive IoT systems. To this end, the notion of local security is investigated, and a PLA scheme is applied to a EPS-AKA protocol

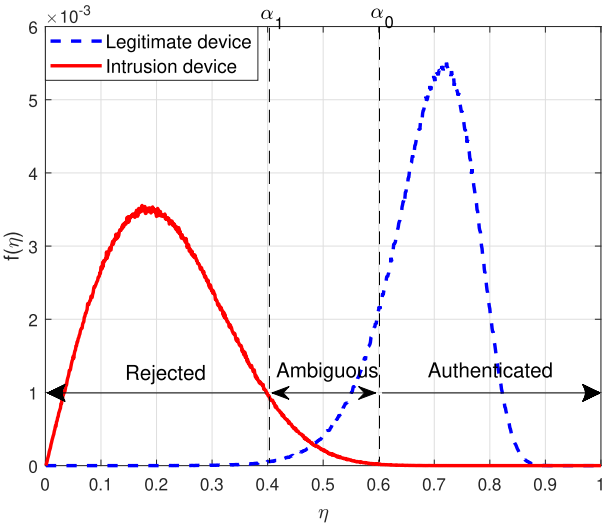


FIGURE 2. Probability density functions of the test statistic, η by legitimate and intrusion signals.

(i.e., LTE model) with the aforementioned integration strategy. Thus, advanced encryption standard (AES), one of the EPS algorithms, is used for encryption and decryption functions in the proposed protocol. In addition, secret keys (i.e., cipher key and integrity key) for cryptography-based security are the same as the conventional EPS-AKA. It is also assumed that both numbers of rounds for PLA and cryptography-based authentication are set to one because we aim to demonstrate the effectiveness of PLA and how to integrate PLA with AKA. Then, a BS plays a crucial role in authenticating an IoT device through a PLA scheme, which further alleviates traffic loads in core networks in the proposed protocol. In PLA, PHY features are exploited to substitute for a secret key or encrypt the secret key for authentication. Then, according to the goal of PHY features in PLA, the proposed protocol is divided into two cases, i.e., 1) without a shared PHY secret key, 2) with a shared PHY secret key.

1) WITHOUT A SHARED PHY SECRET KEY

In this case, PLA without a secret key is applied to a conventional AKA protocol. Thus, the proposed protocol has no use for a PHY secret key; however, it is necessary to register PHY features (e.g., channel, CFO, ...) as a PHY secret key during initial authentication. Here, cryptography-based authentication should be performed for the initial authentication. If successful, PHY features are then estimated and registered by transmitting a pilot signal. Next, based on the shared feature, a PLA scheme is used for preemptive authentication for the subsequent authentications. The flow of the proposed protocol is shown in Fig. 3. As can be seen, 11 messages are divided among three steps: i) initial attach ($M_1^{(1)} \sim M_2^{(1)}$), ii) key generation and distribution ($M_3^{(1)}$)), and iii) authentication ($M_4^{(1)} \sim M_{11}^{(1)}$) messages are exchanged in the proposed protocol as follows.

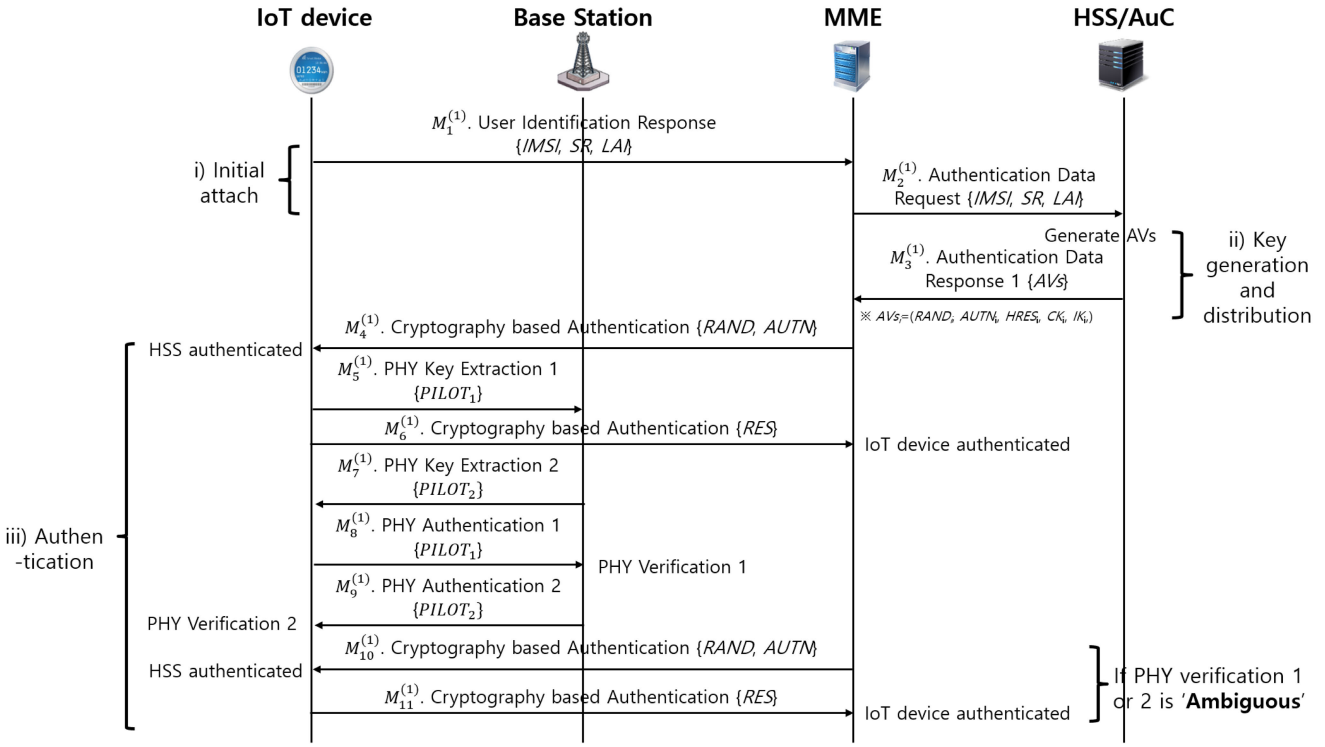


FIGURE 3. Proposed cross-layer authentication protocol without a shared PHY secret key.

- $M_1^{(1)}$: The IoT device sends the IMSI from the universal subscriber identity module (USIM) card of the device for user identification.
- $M_2^{(1)}$: The MME requests authentication data to the HSS by forwarding user identification and network information.
- $M_3^{(1)}$: The HSS generates authentication vectors (AVs) and transmits them to the MME.
- $M_4^{(1)}$: For the initial authentication, the MME selects an AV, retrieves RAND and AUTN, and sends them to the IoT device.
- $M_5^{(1)}$: The IoT device authenticates the networks and transmits a pilot signal to extract PHY features for PLA.
- $M_6^{(1)}$: For the initial authentication of the IoT device, the IoT device transmits RES to the MME.
- $M_7^{(1)}$: The MME authenticates the IoT device and transmits a pilot signal to extract PHY features for PLA.
- $M_8^{(1)}$: For the subsequent authentication, the BS transmits a pilot signal for the authentication using a PLA scheme.
- $M_9^{(1)}$: For the subsequent authentication, the IoT transmits a pilot signal for the authentication using a PLA scheme.
- $M_{10}^{(1)}$: If the PLA result is 'Ambiguous', the MME selects an unused AV, retrieves RAND and AUTN, and sends them to the IoT device.
- $M_{11}^{(1)}$: If the PLA result is 'Ambiguous', the IoT device authenticates the networks and transmits RES to the MME.

Note that the initial authentication procedures differ from those of the subsequent authentications. As mentioned previously, for authentication, PHY features should be extracted in the first authentication process. In addition, AVs for cryptography-based authentication should be generated and distributed in the initial authentication. Then, procedures ($M_1^{(1)} \sim M_7^{(1)}$) are performed for the initial authentication. Furthermore, the registered PHY features at the BS and stored AVs at the MME are used in the subsequent authentications. Then, procedures ($M_1^{(1)}, M_8^{(1)} \sim M_{11}^{(1)}$) are performed in the subsequent authentication. This process determines cryptography-based authentication procedures (M_9 and M_{10}) are required according to the preemptive authentication result.

2) WITH A SHARED PHY SECRET KEY

In this case, a PLA scheme with a secret key is used as preemptive authentication in cross-layer authentication. Here, it is assumed that a PHY secret key is generated and shared to both the HSS and IoT device using the USIM card. Then, unlike the previous case, a PHY feature is used to encrypt the PHY secret key rather than extract the PHY secret key. Thus, from the HSS, the PHY secret key should be distributed to the BS. Then, as shown in Fig. 4, the proposed protocol proceeds as follows.

- $M_1^{(2)}$: Same as $M_1^{(1)}$.
- $M_2^{(2)}$: Same as $M_2^{(1)}$.
- $M_3^{(2)}$: The HSS generates AVs that include a PHY secret key for PLA and transmits them to the MME.

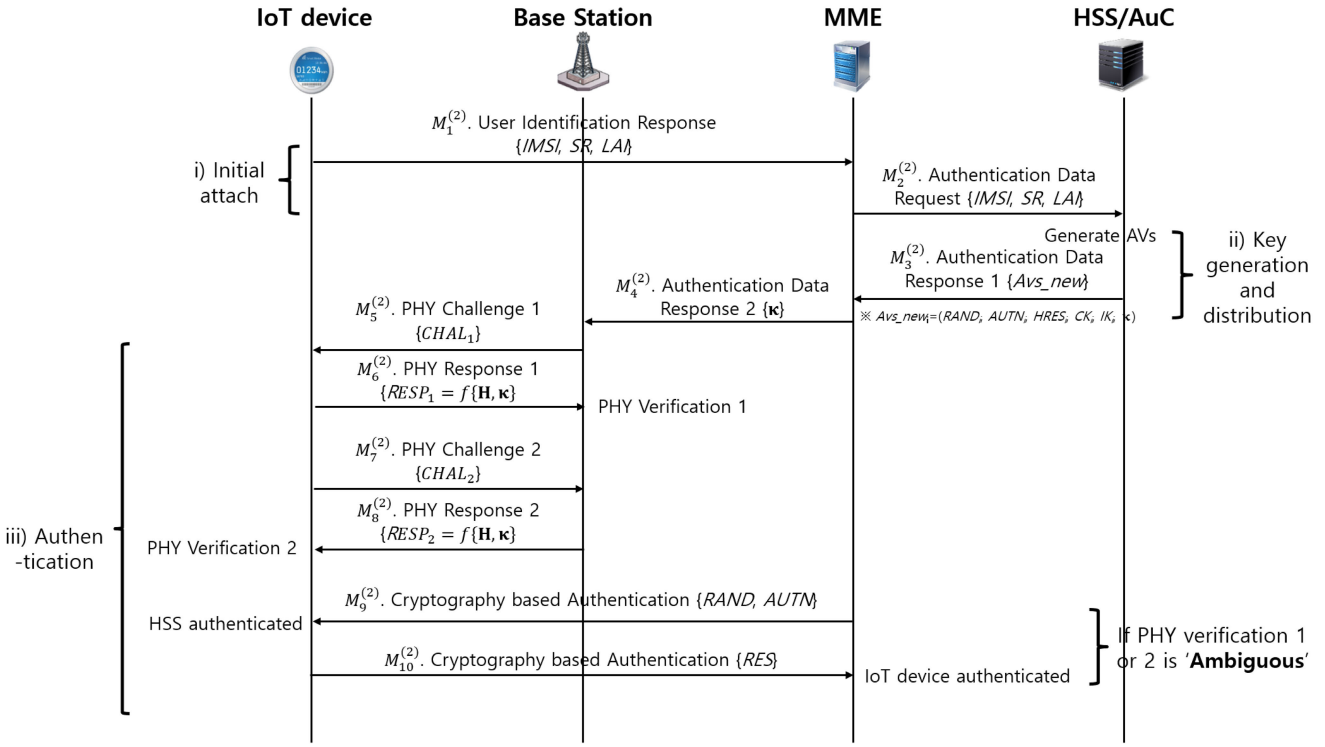


FIGURE 4. Proposed cross-layer authentication protocol with a shared PHY secret key.

- $M_4^{(2)}$: The MME forwards the secret key for the PLA to the BS and retains the other authentication information for cryptographic challenge-response authentication.
- $M_5^{(2)}$: For authentication of the IoT device, the BS transmits a pilot (i.e., challenge) signal to the IoT device.
- $M_6^{(2)}$: The IoT device sends the BS a PHY-response signal with the PHY secret key which is encapsulated with the estimated PHY features.
- $M_7^{(2)}$: For authentication of the network, the IoT device transmits a pilot (i.e., challenge) signal to the BS.
- $M_8^{(2)}$: The BS sends the IoT device a PHY-response signal with the PHY secret key which is encapsulated with the estimated PHY features.
- $M_9^{(2)}$: Same as $M_{10}^{(1)}$.
- $M_{10}^{(2)}$: Same as $M_{11}^{(1)}$.

In this case, for initial authentication, all 10 messages for the three steps are exchanged, whereas seven messages are exchanged for the user identification and authentication procedures (i.e., $M_1^{(2)}, M_5^{(2)} \sim M_{10}^{(2)}$) for the subsequent authentication.

The main difference between the two cases is whether PHY secret key generation and distribution are performed or PHY features are extracted in place of a PHY secret key. Thus, the second case, i.e., with a shared PHY secret key, incurs more signaling overhead than the first case (i.e., without a shared PHY secret key). However, generally, a PLA scheme with a shared PHY secret key (e.g., PHY-CRAM) has better authentication performance than a PLA scheme without a shared PHY secret key. There are two main reasons why the first case shows limited authentication performance improvement over the second case. First, PLA without a shared PHY secret key is more sensitive to communication environment (e.g., noise and interference) because it directly uses physical features (e.g., channel) as a secret key, while PLA with a shared PHY secret key uses the features to encrypt a shared PHY secret key. Thus, the first case is less secure under poor communication environments. Secondly, if the physical features changes rapidly, the first approach can lead to poor authentication performance when the shared PHY secret key is not updated along the channel variations. On the other hand, the second case is less susceptible to channel changes as it uses the instantaneous physical key obtained from the channel when used. For those reasons, PLA without a shared PHY secret key version of the proposed protocol is more suitable for controlled or static environments with less resources. Therefore, two proposed cases can be selectively applied according to the communication scenarios and channel conditions of a wide range of applications in IoT.

IV. PERFORMANCE ANALYSIS

In this section, the proposed protocol is analyzed theoretically in terms of security, overhead, and complexity in massive IoT systems.

A. SECURITY ANALYSIS

The lightweight protocol targets low-cost IoT devices with limited hardware resources; however, it needs to provide reasonable security performance because IoT devices can be

used in CPSs. The proposed cross-layer authentication protocol enhances security against various attacks by exploiting the advantages of both PLA and cryptography-based authentication.

1) EAVESDROPPING ATTACKS

An intruder may try to get a shared PHY secret key via eavesdropping attacks. It is necessary to analyze a formal verification of the proposed protocol against the eavesdropping attacks. However, since this study presents a generalized version of cross-layer authentication without specific security algorithms (e.g. PLA technology and cryptographic algorithms), we cannot strictly verify the security function of the proposed protocol. For formal verification, it is necessary to specify the PLA technique used in the proposed protocol, so for analysis, assume that the proposed protocol uses the PHY-CRAM technique [31]. Then, the response signal encrypted with channel phases is given by [31]

$$s(t) = \sum_{i=1}^{L} \sqrt{\frac{2E_s}{T}} \cos\left(2\pi f_i t + \varphi_i - \Delta\hat{\theta}_{i,1}\right), \tag{4}$$

where $\varphi_i = \frac{1-\kappa_i}{2}\pi$ and $\Delta\hat{\theta}_{i,1}$ is the phase differences between the first and the i-th subcarriers. Here, κ_i is the i-th bit of the secret key. Then, assuming that the intruder IoT device is more than half a wavelength away from the legitimate IoT device and BS, the information-theoretic security of the proposed protocol in an independent fading channel can be verified. Let θ_i and $\tilde{\theta}_i$ denote the i-th channel phases of the legitimate IoT device and the intruder, respectively, and $\theta = \theta_i + \tilde{\theta}_i \mod 2\pi$. In addition, $f_{\theta_i}(x)$, $f_{\tilde{\theta}_i}(x)$, and $f_\theta(x)$ denote the probability density functions (PDFs) of θ_i, $\tilde{\theta}_i$, and θ, respectively. Then, $f_{\theta_i} = \frac{1}{2\pi}$ and $f_{\tilde{\theta}_i} = \frac{1}{2\pi}$, due to Rayleigh fading channels. Thus, since θ_i and $\tilde{\theta}_i$ are independent, the PDF of θ is represented as follows:

$$f_\theta(x) = \int_{-\pi}^{\pi} f_{\theta_i}(x) f_{\tilde{\theta}_i}(x-t)dt = \frac{1}{2\pi}. \tag{5}$$

It means that $\tilde{\theta}_i$ and θ are independent and identically distributed [34]. Then, by monitoring the response signal from the legitimate IoT device, the received signal at the side of an intruder under the noiseless case is given by

$$z(t) = \sum_{i=1}^{L} |g_i| \cos\left(2\pi f_i t + \varphi_i + \theta_1 - (\tilde{\theta}_i - \theta_i)\right), \tag{6}$$

where g_i is the i-th channel coefficient of the intruder. Accordingly, since $\tilde{\theta}_i - \theta_i$ cannot be estimated and is random over $(-\pi, \pi]$, the mutual information between the received signal and the secret key is given by

$$I(\mathbf{z}; \boldsymbol{\kappa}) = 0, \tag{7}$$

where $I(x;y)$ is the mutual information which is a measure of the mutual dependence between x and y. Therefore, it is verified that there is no hope for the intruder to extract any reliable information about the secret key. It means that information theoretic security can be perfectly ensured under the independent Rayleigh fading channel environment.

2) IMPERSONATION ATTACKS

For impersonation attacks, it is assumed that an intrusion IoT device knows which PLA scheme used in the proposed protocol. However, the intrusion device does not know the shared PHY secret key (i.e., $\boldsymbol{\kappa}$) and cannot estimate the PHY features used for authentication. As a result, an arbitrary secret key $\boldsymbol{\kappa}_E$ and its own PHY features are employed for impersonation attacks. Under these conditions, the intrusion IoT device attempts to impersonate a legitimate IoT device. For impersonation attacks, the proposed protocol provides significantly improved authentication reliability compared to conventional PLA. Generally, the miss and false alarm probabilities (denoted P_M and P_F, respectively) are considered to represent the authentication performance of PLA in impersonation attacks. Here, P_M is the probability that the BS will identify the signal as an intrusion signal when a legitimate IoT device transmits, and P_F is the probability that the BS will identify the signal as legitimate when an intrusion device transmits. In conventional PLA, the authentication decision is determined using binary hypothesis testing based on the test statistic η. In detail, using different distributions of η for the hypotheses (i.e., $f_{\eta|\mathcal{H}_1}(x)$ and $f_{\eta|\mathcal{H}_0}(x)$), the BS determines whether the received signal is legitimate or an intrusion with a certain threshold in conventional PLA. Therefore, the differences of the distributions (e.g., Kullback–Leibler (KL) divergence and the difference of cumulative distribution functions (CDFs)) are crucial factors representing PLA performance, where a PLA scheme with large distance between distributions can provide good authentication performance. However, the differences become small in poor communication environments (e.g., environments with significant noise and fading, limited hardware capabilities of an IoT device) regardless of the applied PLA scheme. Thus, the authentication performance of conventional PLA depends on the communication environment, which is an uncontrollable factor. Furthermore, the PHY features of an intrusion IoT device may be similar to those of a legitimate IoT device; however, even under poor conditions, the proposed cross-layer authentication protocol can provide good authentication performance by integrating PLA and cryptography-based authentication. Unlike the single threshold of conventional PLA, here, two thresholds are used to divide the three result cases in the proposed protocol, i.e., 'Rejected', 'Ambiguous' and 'Authenticated'. Note that as mentioned earlier, the two thresholds are determined with target miss and false alarm probabilities (i.e., P_M° and P_F°). Then, we can control the authentication performance with P_M° and P_F°. However, if the P_M° and P_F° values are too small, large signaling overhead can be incurred (Section IV.B).

3) SIGNAL REPLAY ATTACKS

For signal replay attacks, an intrusion IoT device first eavesdrops on an IMSI and authentication signal for PLA

(e.g., $M_9^{(1)}$ and $M_6^{(2)}$), and then attempts to cheat the BS by replaying the identical signal. Here, it is assumed that the intrusion IoT device has sufficient hardware resources. While conventional cryptography-based authentication is difficult in depending on the replay attack, PLA can prevent such attacks using unclonable PHY features (e.g., channel and CFO). First, in a PLA scheme without a shared PHY secret key, a pilot signal (i.e., $M_9^{(1)}$) is transmitted from a legitimate IoT device to estimate the PHY features used for authentication. Then, the intrusion IoT device can easily detect the pilot signal but cannot estimate the PHY features, which are unique due to hardware imperfections and the RF environment, which means that replaying the signal will have no effect. In a PLA scheme with a shared PHY secret key, a response signal (i.e., $M_6^{(2)}$) is transmitted from the legitimate IoT device for authentication. Thus, it is difficult for intrusion IoT device to decode the response signal because the signal is encrypted using PHY features. For example, in PHY-CRAM [31], channel phases are used to encrypt a response signal. As a result, the intrusion IoT device cannot extract reliable information about κ due to the uniqueness of the channel phase. In addition, if the intrusion IoT device replays the received response signal, the BS can discriminate the replayed signal because it is transmitted over a different channel. However, although the intrusion IoT device cannot perfectly estimate and compensate the PHY features, it may compensate some PHY features using intelligent behaviors, e.g., if the intrusion IoT device moves closer to the legitimate IoT device or BS to compensate channels used for authentication. If partial PHY features estimated by the intrusion IoT device are used for replay attacks, the distributions of test statistic (i.e., $f_{\eta|\mathcal{H}_1}(x)$ and $f_{\eta|\mathcal{H}_0}(x)$) get closer. In this case, PLA is vulnerable to replay attacks. In contrast, the proposed protocol is resilient against replay attacks with PHY feature compensation due to the guard interval (i.e., 'Ambiguous') of the proposed integration strategy. Here, there is a high probability that a replayed signal will be included in 'Ambiguous' under PHY feature compensation. Therefore, the signal can be detected via cryptography-based authentication.

4) BRUTE-FORCE ATTACKS

Assuming the intrusion IoT device knows the cryptography-based authentication algorithm, significant effort may be required to extract a secret key used for the algorithm. The existing cryptography-based protocols [9], [11], [14] depend on the computational hardness of encryption algorithms. They can be broken if an intruder has enough computational time and resources. On the other hand, the proposed protocol has not only the computational hardness of cryptography-based authentication but also information-theoretic security induced by PLA. In particular, as physical features (e.g., channel) used for PLA have high independence and randomness each other, the intruder cannot get any information for a secret key although it has enough computational time and resources. In addition, many samples are needed for the cryptography-based authentication signal (e.g., $M_{11}^{(1)}$ and $M_{10}^{(21)}$). In the proposed protocol, it is difficult for the intrusion IoT device to obtain authentication samples because cryptography-based authentication is performed selectively with low probability (Section IV.B), which means that the proposed protocol is secure against other intelligent attacks (e.g., replay and DoS attacks) for cryptography-based authentication.

5) TRACEABILITY ATTACKS

The proposed protocol is vulnerable to a traceability attack since it is designed by integrating PLA with EPS-AKA. However, PLA can be applied to other AKA protocols such as SE-AKA, G-AKA, etc. For example, if a cross-layer authentication protocol integrates PLA with SE-AKA, it can resist the traceability attacks. The traceability attacks are beyond the scope of this study, of which goal is to demonstrate the effectiveness of applying PLA to an AKA protocol by presenting a generalized version of a cross-layer authentication with EPS-AKA.

B. OVERHEAD ANALYSIS

In this subsection, the proposed protocol is analyzed and compared to the conventional EPS-AKA protocol in terms of signaling and communication overheads. As discussed previously, the thresholds (i.e., α_1 and α_0) are determined with P_M° and P_F°, respectively. For convenience, it is assumed that $f_{\eta|\mathcal{H}_1}(x)$ is biased to the right of $f_{\eta|\mathcal{H}_0}(x)$, as shown in Fig. 2. Then, from (3), lower target miss and false alarm probabilities will result in greater distances between α_1 and α_0 which determines the range of 'Ambiguous'. Here, λ denotes a probability of 'Ambiguous' (i.e., $p\,(\alpha_1 \le \eta \le \alpha_0)$); thus, the probability, λ, is given by

$$\begin{aligned}\lambda &= \rho\left(F_{\eta|\mathcal{H}_1}(\alpha_0) - F_{\eta|\mathcal{H}_1}(\alpha_1)\right)\\ &\quad + (1-\rho)\left(F_{\eta|\mathcal{H}_0}(\alpha_0) - F_{\eta|\mathcal{H}_0}(\alpha_1)\right),\\ &= \rho\left(F_{\eta|\mathcal{H}_1}(\alpha_0) - P_M^\circ\right) + (1-\rho)\left(1 - F_{\eta|\mathcal{H}_0}(\alpha_1) - P_F^\circ\right),\\ &= \rho\left(1 - \Delta(\alpha_0) - (P_M^\circ + P_F^\circ)\right)\\ &\quad + (1-\rho)\left(1 - \Delta(\alpha_1) - (P_M^\circ + P_F^\circ)\right), \end{aligned} \tag{8}$$

where ρ is a weighting factor and $\Delta(\alpha) = F_{\eta|\mathcal{H}_0}(\alpha) - F_{\eta|\mathcal{H}_1}(\alpha)$. Here, $\Delta(\alpha)$ is the difference of the cumulative density functions and represents a measure of PLA performance. Then, from (8), as $\Delta(\alpha)$, P_M°, and P_F° increase, low λ values can be obtained in the proposed protocol. This means that, if a PLA scheme integrated with cryptography-based authentication provides good authentication performance, low λ values can be obtained, which produces a small signaling overhead. The relationship between λ and overhead is summarized as follows:

1) SIGNALING OVERHEAD

In [13], the signaling overhead of EPS-AKA is given by

$$\Omega_{EPS-AKA} = N(704 + 608U + 528(P-1)), \tag{9}$$

TABLE 1. Parameters.

Symbol	Descriptions	bits
IMSI	International mobile subscriber identity	128
SR	Service request	8
LAI	Location area identity	40
RES	Response	64
XRES	Expected response	64
CK	Cipher key	128
IK	Integrity key	128
RAND	Random challenge	128
AUTN	Authentication token	160
$\boldsymbol{\kappa}$	PHY secret key	L
$\mathbf{H}$	Channel	L
$PILOT_1$	Pilot signal from IoT device to BS	V
$PILOT_2$	Pilot signal from BS to IoT device	V
$CHAL_1$	Challenge signal from BS to IoT device	L
$CHAL_2$	Challenge signal from IoT device to BS	L
$RESP_1$	Response signal from IoT device to BS	L
$RESP_2$	Response signal from BS to IoT device	L

where N and U are the number of IoT devices and the number of authentication vectors, respectively. In addition, P denotes the number of authentication trials per IoT device.

As shown in Fig. 3, the tenth and the eleventh messages associated with the cryptography-based authentication are exchanged with a probability of $\tilde{\lambda} = 1-(1-\lambda)^2$ for the mutual authentication in the proposed protocol without a shared PHY secret key. Then, the average signaling overhead for the proposed protocol without a shared PHY secret key is given by

$$\begin{aligned}&\mathbb{E}[\Omega_{cross-AKA_1}]\\&= N\left(\left(\sum_{m=1}^{7}|M_m^{(1)}|\right)\right.\\&\quad\left.+(P-1)\left(|M_1^{(1)}|+\sum_{p=8}^{9}|M_p^{(1)}|+\tilde{\lambda}\sum_{q=10}^{11}|M_q^{(1)}|\right)\right),\\&= N\left((704+608U+2V)+(P-1)\left(176+2V+352\tilde{\lambda}\right)\right),\end{aligned}\tag{10}$$

where $M_i^{(1)}$ is the i-th message in the proposed protocol without a shared PHY secret key, and V is the length of the pilot sequence. Based on the related parameters in TABLE 1, $|M_1^{(1)}| = |M_2^{(1)}| = 176$, $|M_3^{(1)}| = 608U$, $|M_4^{(1)}| = 288$ $|M_5^{(1)}| = L$, $|M_6^{(1)}| = 64$, $|M_7^{(1)}| = |M_8^{(1)}| = |M_9^{(1)}| = L$, $|M_{10}^{(1)}| = 288$, and $|M_{11}^{(1)}| = 64$. Similarly, as shown in Fig. 4, the average signaling overhead for the proposed protocol with a shared PHY secret key is given by

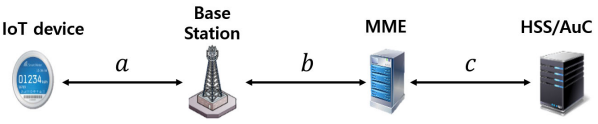


FIGURE 5. Communication costs.

$$\begin{aligned}&\mathbb{E}[\Omega_{cross-AKA_2}]\\&= N\left(\left(\sum_{m=1}^{8}|M_m^{(2)}|+\tilde{\lambda}\sum_{q=9}^{10}|M_q^{(2)}|\right)\right.\\&\quad\left.+(P-1)\left(|M_1^{(2)}|+\sum_{p=5}^{8}|M_p^{(2)}|+\tilde{\lambda}\sum_{q=9}^{10}|M_q^{(2)}|\right)\right),\\&= N\left(\left(352+608U+6L+352\tilde{\lambda}\right)\right.\\&\quad\left.+(P-1)\left(176+4L+352\tilde{\lambda}\right)\right),\end{aligned}\tag{11}$$

where $M_i^{(2)}$ is the i-th message in the proposed protocol with a shared PHY secret key, and L is the length of the PHY secret key. In addition, $|M_1^{(2)}| = |M_2^{(2)}| = 176$, $|M_3^{(2)}| = 608U+L$, $|M_4^{(2)}| = |M_5^{(2)}| = |M_6^{(2)}| = |M_7^{(2)}| = |M_8^{(2)}| = L$, $|M_9^{(2)}| = 288$, and $|M_{10}^{(2)}| = 64$.

The signaling overheads of the proposed protocol depend on L, V and λ determined by P_M°, P_F°, $\Delta(\alpha_0)$, and $\Delta(\alpha_1)$. Then, the signaling overheads in the proposed protocol are less than that of EPS-AKA, when

$$\begin{aligned}\tilde{\lambda} &< 1-\frac{2PV}{352(P-1)}, \quad \text{without a PHY secret key}\\ \tilde{\lambda} &< 1-\frac{(4P+2)L}{352P}, \quad \text{with a PHY secret key.}\end{aligned}\tag{12}$$

Then, from (8), when $\rho = 0.5$, to obtain a small signaling overhead, the PLA scheme for the proposed cross-layer authentication protocol should satisfy the following:

$$\frac{\Delta(\alpha_0)+\Delta(\alpha_1)}{2} \geq 1-\lambda^\circ-\left(P_M^\circ+P_F^\circ\right).\tag{13}$$

Here, λ° denotes a target probability satisfying (12). This means that the signaling overhead in the proposed protocol is affected by own authentication performance of a PLA scheme and target authentication performance.

2) COMMUNICATION OVERHEAD

According to a communication link, the required burden differs for transmission because communication resources (e.g., bandwidth) vary. Here, communication overhead that considers communication cost is more practical than signaling overhead. As shown in Fig. 5, a, b, and c denote cost units incurred by delivering an authentication packet between an IoT device and the BS, between the BS and the MME, and between the MME and HSS, respectively. Then, the communication overhead in EPS-AKA is given by

$$\Lambda_{EPS-AKA} = N\left(495P(a+b)+c(176+608U)\right).\tag{14}$$

Here, $a+b$ is the communication cost between the IoT device and the MME. On the other hand, communication overheads in the proposed protocols without and with the PHY secret key are respectively given by

$$\begin{aligned}
&\mathbb{E}[\Lambda_{cross-AKA_1}] \\
&= N\left(a\left(|M_1^{(1)}| + \sum_{u=4}^{7}|M_u^{(1)}|\right)\right. \\
&\quad + b\left(|M_1^{(1)}| + |M_4^{(1)}| + |M_6^{(1)}|\right) + c\sum_{m=2}^{3}|M_m^{(1)}| \\
&\quad + (P-1)\left(a\left(|M_1^{(1)}| + \sum_{p=8}^{9}|M_p^{(1)}| + \tilde{\lambda}\sum_{q=10}^{11}|M_q^{(1)}|\right)\right. \\
&\quad \left.\left. + b\left(|M_1^{(1)}| + \tilde{\lambda}\sum_{q=10}^{11}|M_q^{(1)}|\right)\right)\right), \\
&= N(a(528+2V) + 528b + c(176+608U) \\
&\quad + (P-1)(a(176+2V+352\tilde{\lambda}) + b(176+352\tilde{\lambda}))).
\end{aligned} \tag{15}$$

and

$$\begin{aligned}
&\mathbb{E}[\Lambda_{cross-AKA_2}] \\
&= \left(a\left(|M_1^{(2)}| + \sum_{i=5}^{8}|M_i^{(2)}| + \tilde{\lambda}\sum_{j=9}^{10}|M_j^{(2)}|\right)\right. \\
&\quad + b\left(|M_1^{(2)}| + |M_4^{(2)}| + \tilde{\lambda}\sum_{j=9}^{10}|M_j^{(2)}|\right) + c\sum_{m=2}^{3}|M_m^{(2)}| \\
&\quad + (P-1)\left(a\left(|M_1^{(2)}| + \sum_{i=5}^{8}|M_i^{(2)}| + \tilde{\lambda}\sum_{j=9}^{10}|M_j^{(2)}|\right)\right. \\
&\quad \left.\left. + b\left(|M_1^{(2)}| + \tilde{\lambda}\sum_{j=9}^{10}|M_j^{(2)}|\right)\right)\right)N, \\
&= N(a(176+4L+352\tilde{\lambda}) + b(176+L+352\tilde{\lambda}) \\
&\quad + c(176+608U+L) + (P-1)(a(176+4L+352\tilde{\lambda}) \\
&\quad + b(176+352\tilde{\lambda}))).
\end{aligned} \tag{16}$$

From (14) and (15), the communication overhead of the proposed protocol without a shared PHY secret key is less than that of EPS-AKA when

$$\Delta_{A,1}a > \Delta_{B,1}b, \tag{17}$$

where $\Delta_{A,1} = 352(P-1)(1-\tilde{\lambda}) - 2PV$ and $\Delta_{B,1} = 352(P-1)(\tilde{\lambda}-1)$. Then, for any c, the proposed protocol without a shared PHY secret key and the EPS-AKA are affected equally. Furthermore, a large b value is favorable in the proposed protocol without a shared PHY secret key because $\Delta_{B,1} < 0$. In addition, if $V < -\frac{\Delta_{B,1}}{2P}$, the proposed protocol without a shared PHY secret key always has less communication overhead than EPS-AKA regardless of the cost units (i.e., a and b).

TABLE 2. Time cost parameters.

Description	Cost time
Hash time in IoT device (T_{H-IoTD})	0.0365 ms
Hash time in MME (T_{H-MME})	0.0121 ms
Hash time in HSS (T_{H-HSS})	0.0121 ms
Point multiplication time in IoT device (T_{M-IoTD})	1.53 ms
Point multiplication time in MME (T_{M-MME})	0.475 ms
Point multiplication time in HSS (T_{M-HSS})	0.475 ms
Lagrange component time in IoT device (T_{L-IoTD})	0.0572 ms
Lagrange component time in HSS (T_{L-HSS})	0.0351 ms

In the same manner, from (14) and (16), if $L < \frac{(1-\tilde{\lambda})352}{4}$, the communication overhead in the proposed protocol with a shared PHY secret key is less than that of EPS-AKA when the following condition is satisfied:

$$a > \frac{\left(352P(\tilde{\lambda}-1)+L\right)b + Lc}{P\left((1-\tilde{\lambda})352 - 4L\right)}. \tag{18}$$

Furthermore, if $b = c$, it can be represented as follows:

$$\frac{a}{b} > \frac{352P(\tilde{\lambda}-1)+352}{P((1-\tilde{\lambda})352-4L)}. \tag{19}$$

From our analyses, we found that the proposed protocol without a shared PHY secret key demonstrates better performance than the method with a shared PHY secret key in terms of communication overhead if $L = V$.

C. COMPLEXITY ANALYSIS

In this subsection, the computational complexity of the proposed protocol is analyzed. The time used for primitive operations was measured using the C/C++ OPENSSL library [41] tested on a Celeron 1.1 GHz processor as a IoT device and Dual-core 2.6 GHz CPU as an MME and HSS. Here, we set the time cost parameters (TABLE 2) in reference to [42].

Unlike conventional cryptography-based schemes, a PLA scheme requires extra computation using PHY features rather than encryption algorithms (e.g., a hash algorithm). However, the feature estimation (e.g., channel and CFO estimations) is necessary for wireless communications (not for authentication). This means that extra estimation resources are not required for authentication in the proposed protocol.

The mean of computation time of the proposed protocol is calculated as follows:

$$\mathbb{E}[\Psi_{cross}] = 5\lambda N(T_{H-IoTD} + T_{H-HSS}), \tag{20}$$

where T_{H-IoTD} and T_{H-HSS} denote the hash time in IoT device and in HSS, respectively. Then, the computation time of the proposed protocol is very short due to the small λ values. As shown in Table 3, the proposed protocol has very short computation time compared to existing AKA protocols,

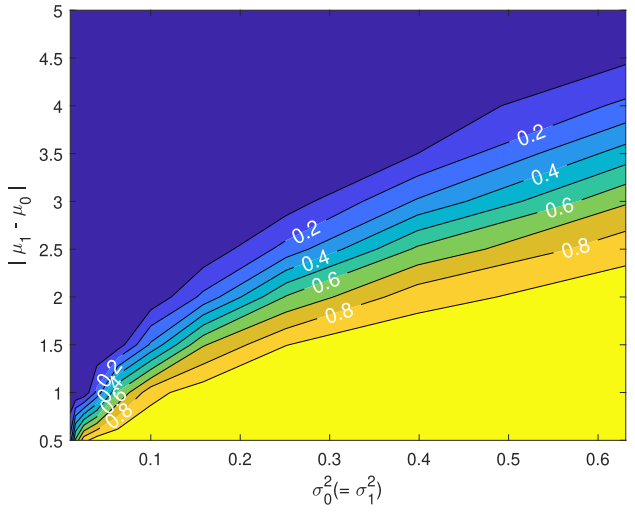


FIGURE 6. False alarm probability for various $|\mu_1 - \mu_0|$ and σ_0^2, where $\sigma_1^2 = \sigma_0^2$, and $P_M^\circ = 10^{-5}$.

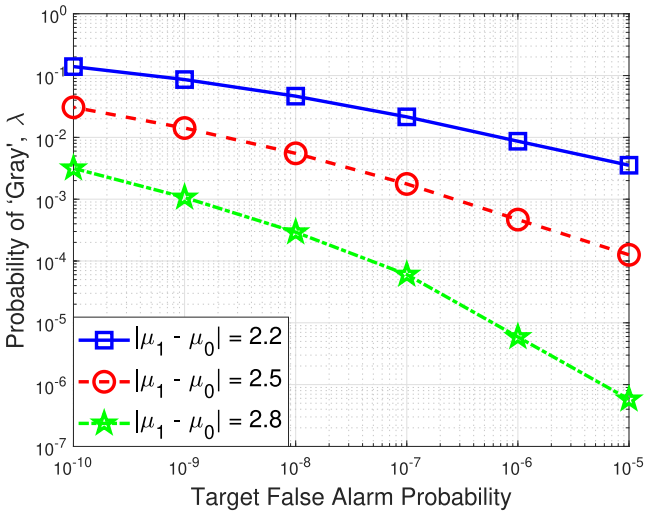


FIGURE 7. λ for different target false alarm probabilities, where $P_M^\circ = 10^{-5}$, $\rho = 0.5$, $\mu_0 = 0$, and $\sigma_0^2 = \sigma_1^2 = 0.1$.

where C denotes the number of groups for group-based AKA algorithms.

V. SIMULATION RESULTS

In this section, we present simulation results to discuss the performance of the proposed protocol in terms of authentication, overhead, and computational complexity. For these simulations, we assumed that the distributions of η for legitimate and intrusion signals follow Gaussian distributions with means of μ_0 and μ_1 and variances of σ_0^2 and σ_1^2, respectively. Here, $\Delta(\alpha) = \frac{1}{2}\left(\text{erf}\left(\frac{\alpha-\mu_0}{\sigma_0\sqrt{2}}\right) - \text{erf}\left(\frac{\alpha-\mu_1}{\sigma_2\sqrt{2}}\right)\right)$ which is the difference of two CDFs for legitimate and intrusion IoT signals. Note that the difference of two CDFs represents the authentication performance of a PLA scheme. Meanwhile, units of signaling and communication overheads are bit. In addition, it is assumed that $a = 1/BW_a$, $b = 1/BW_b$, and $c = 1/BW_c$, where BW_a, BW_b, and BW_c denote the bandwidths between IoT device and BS and between BS and MME and between MME and HSS, respectively. Here, we set $BW_a = 2 \times 10^5$ and $BW_b = BW_c = 3.55 \times 10^8$ because the RF bandwidth of NB-IoT is 200 kHz [43] and control plane interfaces for connections between BS and MME and between MME and HSS in NB-IoT require minimum bandwidth of 0.355 GHz [44].

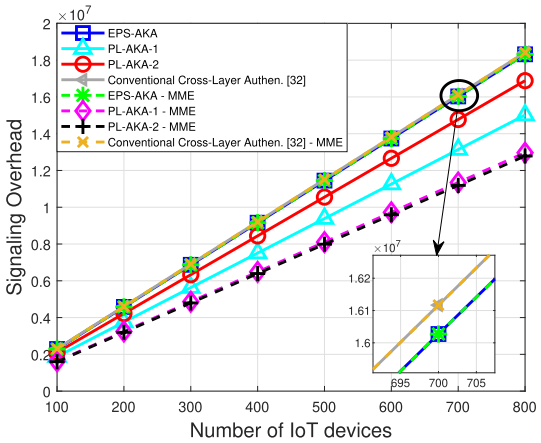
In Fig. 6, we show the false alarm probability for various $|\mu_1 - \mu_0|$ and σ_0^2, where $\sigma_1^2 = \sigma_0^2$, and $P_M^\circ = 10^{-5}$. As mentioned previously, $\Delta(\alpha)$ which represents the authentication performance of PLA is determined by distributions of test statistic. Thus, it is necessary to analyze the impact of key indicators (e.g., mean and variance) for the distributions on authentication performance. From this figure, it is demonstrated that as the difference between μ_0 and μ_1 increases and σ_0^2 decreases, the PLA scheme has an improved authentication performance. Here, the parameters of distributions (i.e., μ_0, μ_1, σ_0^2, and σ_1^2) depend on not only which PLA scheme we use but also communication environment (e.g., SNR). So, it is difficult for PLA to guarantee good authentication performance under poor communication environment.

In Fig. 7, we show the relationship between λ and P_F° in the proposed protocol, where $P_M^\circ = 10^{-5}$, $\rho = 0.5$, $\mu_0 = 0$, and $\sigma_0^2 = \sigma_1^2 = 0.1$. First, as seen in the figure, for a fixed target false alarm probability, the target false alarm probability, P_F°, is inversely proportional to λ. That is, high target miss and false alarm probabilities make the distance between two thresholds (i.e., α_0 and α_1) narrow. As a result, the probability of 'Ambiguous' becomes low because the distance is the range of 'Ambiguous' (from (3)). In addition, it is favorable to have a large $|\mu_1 - \mu_0|$ because the probability density functions of $\eta|\mathcal{H}_i$ are distant from each other with a large $|\mu_1 - \mu_0|$. This implies that if the authentication performance of the PLA is improved, signaling overhead can be reduced in the proposed protocol with a low λ.

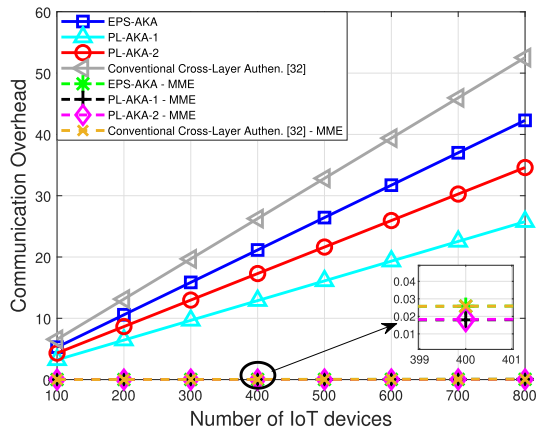
Fig. 8 shows the simulation results for the signaling and communication overheads over various numbers of IoT devices to compare the proposed protocol to conventional AKA and cross-layer authentication protocols [34], where $P = 20$, $U = 20$, $L = V = 64$, and $\lambda = 10^{-5}$. In these simulations, total overhead and overhead at the MME were considered. The overhead at the MME is the overhead of messages exchanged at the MME. As shown in the figure, the proposed protocol demonstrates small total signaling and communication overheads compared to the conventional EPS-AKA and cross-layer authentication protocol [34]. In addition, the proposed protocol without a shared PHY secret key shows slightly improved performance compared to the proposed protocol with a shared PHY secret key in terms of signaling and communication overheads due to the simple procedures of PLA without a shared PHY secret key. Furthermore, while the signaling overhead at the MME is the same as the total signaling overhead in the conventional protocols, in the proposed protocol, the signaling overhead at the MME is significantly less than the total signaling

TABLE 3. Computation time of AKA protocols.

	EPS-AKA [16]	SE-AKA [9]	S-AKA [14]	G-AKA [11]	Proposed protocol
First IoT device	0.178	3.2964	0.2136	0.1424	$0.178\tilde{\lambda}$
Remaining IoT devices	$0.178(N-1)$	$3.2608(N-1)$	$0.2136(N-1)$	$0.1424(N-1)$	$0.178\tilde{\lambda}(N-1)$
BS	0	0	0	0	0
MME	0	$0.9863N$	$0.0242N$	$0.363N$	0
HSS	$0.0605N$	$0.242C$	$0.242N$	$0.242C$	$0.0604N\tilde{\lambda}$
Total	$0.235N$	$4.2471N+0.0242C$	$0.262N$	$0.1787N+0.0242C$	$0.235N\tilde{\lambda}$

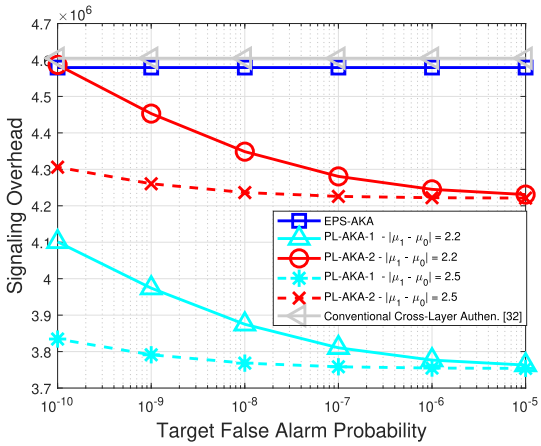


(a) Signaling overhead

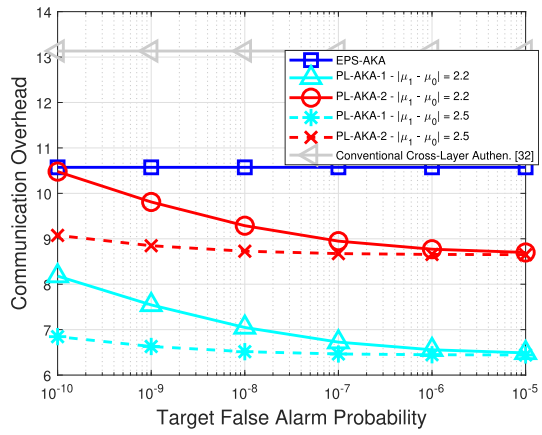


(b) Communication overhead

FIGURE 8. Overhead over various numbers of IoT devices, where $P = 20$, $U = 20$, $L = V = 64$, and $\lambda = 10^{-5}$.



(a) Signaling overhead

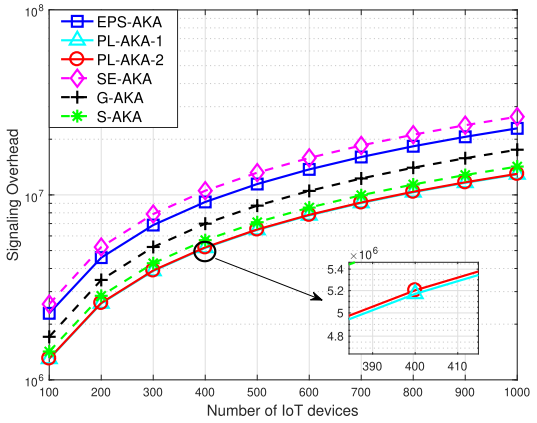


(b) Communication overhead

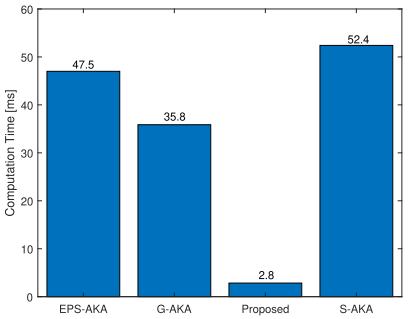
FIGURE 9. Overhead over various target false alarm probabilities, where $\mu_0 = 0$, $\sigma_0^2 = \sigma_1^2 = 0.1$, $P_M^\circ = 10^{-5}$, $P = 20$, $U = 20$, $L = V = 64$, and $N = 200$.

overhead because, in the proposed protocol, the BS performs preemptive authentication (i.e., PLA) rather than the MME.

In Fig. 9, the signaling and communication overheads are plotted for different target false alarm probabilities to demonstrate the relationship between authentication performance and overhead, where $\mu_0 = 0$, $\mu_1 = 2.5$, $\sigma_0^2 = \sigma_1^2 = 0.1$, $P_M^\circ = 10^{-5}$, $P = 20$, $U = 20$, $L = 64$, and $N = 200$. As seen the figures, as a false alarm probability increases, signaling and communication overheads slightly decrease due to the inverse proportional relationship between and P_F° and λ (In details, please see Fig. 7). It means that there is a trade-off between authentication performance and signaling overhead. For example, if we set threshold values, i.e., α_0 and α_1, which make target miss and false alarm probabilities low to enhance the security, the proposed protocol will require more overhead with a large λ. Fortunately, however, although a false alarm probability is very low (e.g., $P_F^\circ = 10^{-10}$), the proposed



(a) Signaling overhead



(b) Computation time, where $N = 200$.

FIGURE 10. Signaling overhead and computation time to compare the proposed protocol to the conventional AKA protocols [9], [11], [14], where $\mu_0 = 0$, $\mu_1 = 2.5$, $\sigma_0^2 = \sigma_1^2 = 0.1$, $P_M^\circ = 10^{-5}$, $P_F^\circ = 10^{-10}$, $P = 20$, $U = 20$, $L = V = 64$, and $C = 5$.

protocol maintains small signaling and communication overheads compared to the conventional EPS-AKA. Furthermore, the proposed protocol can improve the performances with a large difference of distributions (i.e., $|\mu_1 - \mu_0|$) in terms of signaling and communication overheads. That is, if a PLA scheme which provides a good authentication performance is used in the proposed protocol, signaling and communication overhead can be reduced with fixed target miss and false alarm probabilities.

Fig. 10 shows the simulation results for signaling overhead and computation time to compare the proposed protocol to the conventional AKA protocols [9], [11], [14], where $\mu_0 = 0$, $\mu_1 = 2.5$, $\sigma_0^2 = \sigma_1^2 = 0.1$, $P_M^\circ = 10^{-5}$, $P_F^\circ = 10^{-10}$, $P = 20$, $U = 20$, $L = V = 64$, and $C = 5$. As shown in the Fig. 10 (a), the proposed protocol outperforms conventional lightweight AKA protocols [9], [11], [14] in terms of signaling overhead. In addition, if the proposed protocol is designed by applying PLA to the lightweight AKA protocols, the signaling overhead is expected to be further reduced. Meanwhile, from (20), the computational complexity is inversely proportional to authentication performance (i.e., miss and false alarm probabilities) due to the proportional relationship between λ and computation time. However, as seen in Fig. 10 (b), the proposed protocol outperforms conventional lightweight AKA protocols in terms of computation time under the sufficiently low false alarm probability (i.e., $P_F^\circ = 10^{-10}$). It means that the proposed protocol is suitable for the authentication of IoT devices which have limited hardware resources.

VI. CONCLUSION

In this article, we have proposed a cross-layer authentication protocol to reduce signaling overhead in massive IoT systems. By exploiting the notion of local security, PLA is employed as preemptive authentication between IoT devices and a BS. Based on our integration strategy, cryptography-based authentication is performed selectively using the preemptive PLA result to reduce signaling overhead. The proposed protocol is divided into two cases, without and with an additional secret key. We analyzed the signaling and communication overheads of the proposed methods for a target authentication performance. Meanwhile, a required authentication performance of a PLA scheme is derived for target authentication and overhead performances. Through theoretical analysis and numerical simulations, we have demonstrated that the proposed protocol incurs less overhead and has smaller computational complexity than conventional AKA protocols while maintaining competitive authentication performance.

There are several avenues in which to explore this research further. First, it is worth discussing how to find optimal thresholds which maximize a trade-off between authentication performance and overhead in the proposed protocol. In addition, PLA that employs multiple physical features should be considered to improve authentication performance of the proposed protocol in future.

REFERENCES

[1] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, Jun. 2017.

[2] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[3] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[4] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, "Efficient authentication and key distribution in wireless IP networks," *IEEE Wireless Commun.*, vol. 10, no. 6, pp. 52–61, Dec. 2003.

[5] C. B. Sankaran, "Network access security in next- generation 3GPP systems: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 84–91, Feb. 2009.

[6] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 283–302, 1st Quart., 2014.

[7] I. Gharsallah, S. Smaoui, and F. Zarai, "An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks," *IET Inf. Secur.*, vol. 14, no. 1, pp. 21–29, Jan. 2020.

[8] J. Cao, M. Ma, and H. Li, "LPPA: Lightweight privacy-preservation access authentication scheme for massive devices in fifth generation (5G) cellular networks," *Wiley Int. J. Commun. Syst.*, vol. 32, no. 3, pp. 1–24, Feb. 2019.

[9] C. Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Comput. Netw.*, vol. 57, no. 17, pp. 3492–3510, Dec. 2013.

[10] J. Cao, M. Ma, and H. Li, "A group-based authentication and key agreement for MTC in LTE networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 1017–1022.

[11] Y. Chen, J. Wang, K. Chi, and C. Tseng, "Group-based authentication and key agreement," *Wireless Pers. Commun.*, vol. 62, no. 4, pp. 965–979, Feb. 2012.

[12] 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.

[13] C. Lai, H. Li, X. Li, and J. Cao, "A novel group access authentication and key agreement protocol for machine-type communication," *Trans. Emerg. Telecommun. Technol.*, vol. 26, no. 3, pp. 414–431, Mar. 2015.

[14] Y.-L. Huang, C.-Y. Shen, and S. W. Shieh, "S-AKA: A provable and secure authentication key agreement protocol for UMTS networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 9, pp. 4509–4519, Nov. 2011.

[15] M. M. Modiri, J. Mohajeri, and M. Salmasizadeh, "GSL-AKA: Group-based secure lightweight authentication and key agreement protocol for M2M communication," in *Proc. 9th Int. Symp. Telecommun. (IST)*, Dec. 2018, pp. 275–280.

[16] *3G System Architecture Evolution (SAE); Security Architecture (Release 8)*, document TS 33.401 V8.2.1, 3GPP, 2009.

[17] M. A. Abdrabou, A. D. E. Elbayoumy, and E. A. El-Wanis, "LTE authentication protocol (EPS-AKA) weaknesses solution," in *Proc. IEEE 7th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS)*, Dec. 2015, pp. 434–441.

[18] P. E. Abi-Char, P. Nader, and S. Mahfouz, "A secure and lightweight authenticated key agreement protocol for distributed IoT applications," in *Proc. 43rd Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2020, pp. 50–56.

[19] M. Tanveer, A. H. Zahid, M. Ahmad, A. Baz, and H. Alhakami, "LAKE-IoD: Lightweight authenticated key exchange protocol for the Internet of drone environment," *IEEE Access*, vol. 8, pp. 155645–155659, 2020.

[20] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[21] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.

[22] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[23] C. Pei, N. Zhang, X. S. Shen, and J. W. Mark, "Channel-based physical layer authentication," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 4114–4119.

[24] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, Jul. 2012.

[25] A. Ferrante, N. Laurenti, C. Masiero, M. Pavon, and S. Tomasin, "On the error region for channel estimation-based physical layer authentication over Rayleigh fading," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 941–952, May 2015.

[26] 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.

[27] 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.

[28] M. Pospíšil and R. Maršálek, "Experimental study of wireless transceiver authentication using carrier frequency offset monitoring," in *Proc. 25th Int. Conf. Radioelektronika (RADIOELEKTRONIKA)*, Apr. 2015, pp. 335–338.

[29] Y. Lee, E. Hwang, and J. Choi, "A unified approach for compression and authentication of smart meter reading in AMI," *IEEE Access*, vol. 7, pp. 34383–34394, 2019.

[30] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, Sep. 2013.

[31] X. Wu and Z. Yang, "Physical-layer authentication for multi-carrier transmission," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 74–77, Jan. 2015.

[32] X. Wu, Z. Yang, C. Ling, and X.-G. Xia, "Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6611–6625, Oct. 2016.

[33] H. Wen, Y. Wang, L. Zhou, X. Zhu, and J. Li, "Physical layer assist authentication technique for smart meter system," *IET Commun.*, vol. 7, no. 3, pp. 189–197, Feb. 2013.

[34] X. Wu, Z. Yan, C. Ling, and X.-G. Xia, "Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission," 2015, *arXiv:1502.07565*. [Online]. Available: http://arxiv.org/abs/1502.07565

[35] H. Park, H. Roh, and W. Lee, "Tagora: A collision-exploitative RFID authentication protocol based on cross-layer approach," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3571–3585, Apr. 2020.

[36] Z. Zhao, Y. Hou, X. Tang, and X. Tao, "Demo abstract: Cross-layer authentication based on physical channel information using OpenAirInterface," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 1334–1335.

[37] Z. Zhang, N. Li, S. Xia, and X. Tao, "Fast cross layer authentication scheme for dynamic wireless network," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6.

[38] P. Hao, X. Wang, and W. Shen, "A collaborative PHY-aided technique for end-to-end IoT device authentication," *IEEE Access*, vol. 6, pp. 42279–42293, 2018.

[39] Y. Lee, E. Hwang, and J. Choi, "Physical layer aided authentication and key agreement for the Internet of Things," in *Proc. 14th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, 2020.

[40] *3G System Architecture Evolution (SAE); Security Architecture (Release 13)*, document TS 33.401 V13.2.0, 3GPP, 2016.

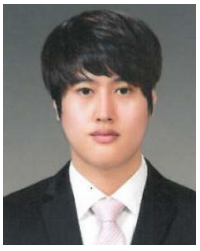
[41] J. Viega, M. Messier, and P. Chandra, *Network Security With OpenSSL: Cryptography for Secure Communications*. Sebastopol, CA, USA: O'Reilly Media, 2002.

[42] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A simple and robust handover authentication between HeNB and eNB in LTE networks," *Comput. Netw.*, vol. 56, no. 8, pp. 2119–2131, May 2012.

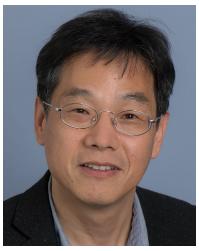
[43] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band Internet of Things," *IEEE Access*, vol. 5, pp. 20557–20577, 2017.

[44] A. Hikmaturokhman, L. S. Palupi, N. Amalia, A. R. Danisya, and T. A. Nugraha, "4G LTE evolved packet core planning with call switch fallback technology," *J. Telecommun., Electron. Comput. Eng.*, vol. 10, nos. 1–6, pp. 133–136, 2018.

YONGGU LEE received the B.E. degree in electronics engineering from Kyungpook National University, Daegu, South Korea, in 2013, and the M.S. and Ph.D. degrees in electrical engineering and computer science from the Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, in 2016 and 2019, respectively. He was with the Research Institute for Solar and Sustainable Energies, GIST, from 2019 to 2020. Since 2020, he has been a Senior Researcher with the Security Research and Development Team, Korea Atomic Energy Research Institute (KAERI), South Korea. His research interests include anti-drone system, wireless communications and signal processing, with emphasis on physical layer security, 5G communication systems, and machine type communications.



JISEOK YOON (Graduate Student Member, IEEE) received the B.E. degree in electronics engineering from the Kumoh National Institute of Technology, Gumi, South Korea, in 2012, and the M.S. degree in mechatronics from the Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, in 2014, where he is currently pursuing the Ph.D. degree. His research interests include signal processing and machine learning, with emphasis on image, smart grid, and security fields.



JINHO CHOI (Senior Member, IEEE) was born in Seoul, South Korea. He received the B.E. degree *(magna cum laude)* in electronics engineering from Sogang University, Seoul, in 1989, and the M.S.E. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), in 1991 and 1994, respectively. He is currently with the School of Information Technology, Burwood, Deakin University, Australia, as a Professor. Prior to joining Deakin in 2018, he was with Swansea University, U.K., as a Professor/Chair of wireless, and the Gwangju Institute of Science and Technology (GIST), Korea, as a Professor. His research interests include the Internet of Things (IoT), wireless communications, and statistical signal processing. He has authored two books published by Cambridge University Press in 2006 and 2010. He received the 1999 Best Paper Award for Signal Processing from EURASIP and the 2009 Best Paper Award from WPMC (Conference). He is an Editor of IEEE TRANSACTIONS COMMUNICATIONS and the IEEE WIRELESS COMMUNICATIONS LETTERS and a Division Editor of *Journal of Communications and Networks* (JCN). He has served as an Associate Editor or Editor of other journals including the IEEE COMMUNICATIONS LETTERS, JCN, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and *ETRI* journal.

EUISEOK HWANG (Member, IEEE) received the B.S. and M.S. degrees from the School of Engineering, Seoul National University, Seoul, South Korea, in 1998 and 2000, respectively, and the M.S. and Ph.D. degrees in electrical and computer engineering from Carnegie Mellon University, Pittsburgh, PA, USA, in 2010 and 2011, respectively. He was with the Digital Media Research Center, Daewoo Electronics Co., Ltd., South Korea, from 2000 to 2006, and was with the Channel Architecture Group, LSI Corporation (currently Broadcom), San Jose, CA, USA, from 2011 to 2014. Since 2015, he has been an Assistant/Associate Professor with the School of Mechatronics/Electrical Engineering and Computer Science /Artificial Intelligence, Gwangju Institute of Science and Technology (GIST), South Korea. He holds over 20 granted U.S. patents and over 100 journal articles and conference papers in information and signal processing area. His research interests include data channel signal processing and coding, energy informatics and intelligence implementations for smart grid, and information processing for system intelligence in emerging ICT/IoT applications.