

Article

Lightweight Physical Layer Aided Key Agreement and Authentication for the Internet of Things[†]

Seungnam Han¹ , Yonggu Lee² , Jinho Choi³  and Euseok Hwang^{1,*} 

¹ School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology (GIST), Gwangju 61005, Korea; snhan0911@gm.gist.ac.kr

² Security Research and Development Team, Korea Atomic Energy Research Institute (KAERI), Daejeon 34057, Korea; ygl@kaeri.re.kr

³ School of Information Technology, Deakin University, Geelong, VIC 3220, Australia; jinho.choi@deakin.edu.au

* Correspondence: euseokh@gist.ac.kr

[†] This paper is an extended version of our paper published in Lee, Y.; Choi, J.; Hwang, E. Physical Layer Aided Authentication and Key Agreement for the Internet of Things. In Proceedings of the 14th International Conference on Signal Processing and Communication Systems (ICSPCS'2020), Adelaide, Australia, 14–16 December 2020.

Abstract: In this paper, we propose a lightweight physical layer aided authentication and key agreement (PL-AKA) protocol in the Internet of Things (IoT). The conventional evolved packet system AKA (EPS-AKA) used in long-term evolution (LTE) systems may suffer from congestion in core networks by the large signaling overhead as the number of IoT devices increases. Thus, in order to alleviate the overhead, we consider cross-layer authentication by integrating physical layer approaches to cryptography-based schemes. To demonstrate the feasibility of the PL-AKA, universal software radio peripheral (USRP) based tests are conducted as well as numerical simulations. The proposed scheme shows a significant reduction in the signaling overhead, compared to the conventional EPS-AKA in both the simulation and experiment. Therefore, the proposed lightweight PL-AKA has the potential for practical and efficient implementation of large-scale IoT networks.

Keywords: authentication and key agreement; Internet of Things; physical layer authentication; universal software radio peripheral



Citation: Han, S.; Lee, Y.; Choi, J.; Hwang, E. Light-Weight Physical Layer Aided Key Agreement and Authentication for the Internet of Things. *Electronics* **2021**, *10*, 1730. <https://doi.org/10.3390/electronics10141730>

Academic Editor: Tadeusz A. Wysocki

Received: 30 June 2021

Accepted: 15 July 2021

Published: 19 July 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In recent years, the application of the Internet of Things (IoT) has become a part of our daily life, and the number of IoT devices is growing rapidly, accordingly. The number of connected devices is expected to reach 500 billion by 2030, which is approximately 59 times the projected global population [1]. Moreover, the growth is expected to continue with massive IoT (MIoT) developments as fifth-generation (5G) wireless communications are deployed in a variety of applications. For this reason, wireless security has also become one of the major concerns, due to the broadcast nature of radio signals. For example, they are vulnerable to spoofing attacks, where a malicious user impersonates a legitimate user.

For this reason, an evolved packet system authentication and key agreement (EPS-AKA) protocol has been widely used for mutual authentication between a cellular network and a mobile device in long-term evolution (LTE) systems [2]. However, MIoT systems with hardware and resource limitations can introduce large signal overheads and long delays. Thus, lightweight AKA algorithms have been studied for a large number of IoT devices in [3–5]. In [5], group-based AKA (G-AKA) protocols that enable simultaneous authentication of a good deal of IoT devices are proposed, but G-AKA schemes are difficult to overcome the single secret key agreement limitation caused by the simultaneous authentication and susceptibility to identified attacks. Instead, physical layer authentication (PLA) has been studied for the authentication of IoT devices with low complexity and

fast authentication [6,7]. In particular, a physical layer challenge-response authentication mechanism (PHY-CRAM) [8–10] exploits characteristics of the physical channel to conceal the authentication key, preventing eavesdroppers from impersonating based attacks. However, PLA is inherently difficult to guarantee authentication performance in poor communication environments. As in [11–14], cross-layer authentication schemes integrate PLA to cryptography-based authentication in order to compensate PLA, but simply cascading both layer schemes might be inefficient to apply in practical application due to the limited resources of the networks.

In this paper, we consider a lightweight physical layer aided authentication and key agreement (PL-AKA) protocol for MIoT environments, providing a favorable balance between the signal overhead and reliability by selectively applying conventional cryptography-based authentication along with PLA and preliminary PLA decisions. To demonstrate the effectiveness of the proposed protocol, an experimental analysis is performed with a universal software radio peripheral (USRP). The main contributions of this paper are summarized as follows:

- For sophisticated cross-layer authentication, we propose a novel integration strategy based on the test statistic result of the PHY-CRAM. By using this integration strategy, a proposed protocol can reduce the signaling overhead, while providing a competitive authentication performance. This is the main difference with existing cross-layer authentication protocols based on simple concatenation and encapsulation operations [11–14].
- For the performance analysis, we analyze the authentication error probability and signaling overhead of the proposed protocol.
- For the validation of PLA in the proposed protocol, an RF experiment is conducted with USRP transceivers.

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

2. Motivation and Local Security

In 5G networks, supporting the high concurrent connections of many low-cost devices is very important. International mobile telecommunication (IMT) expects massive access of at least 1 million devices per squared kilometer to be supported in 5G networks [15]. As such, 5G should cover densely populated areas, such as residential buildings or business centers in urban environments [16], where a large signaling overhead induced by conventional cryptographic authentication mechanisms may cause inevitable delays. Furthermore, when massive devices access 5G networks simultaneously, severe signaling congestion can be incurred over the network nodes, such as mobility management entity (MME) and home subscriber server (HSS) because of the conventional centralized security managed at the core networks. Alternatively, a new security architecture, which imposes a burden of security (i.e., authentication) into radio access networks (RANs) in a distributed manner is considered in this paper, referred to as a local security. A base station (BS) in RANs authenticates IoT devices on its own to reduce the excessive network traffic to the MME in the local security. Meanwhile, PLA is suitable for IoT devices, due to its fast authentication with low computational complexity. So, PLA employs authentication between a BS and an IoT device to reduce burden at a BS. However, as mentioned earlier, PLA methods may have poor authentication performance under bad communication conditions (e.g., low signal-to-noise ratio (SNR) and correlated channels). Thus, a cross-layer authentication protocol that integrates PLA in RANs and cryptography-based authentication in core networks is considered. However, conventional cross-layer authentication protocols [11–14] cannot provide both reliable authentication performance and a small signaling overhead for 5G networks. For example, as mentioned earlier, the authentication protocol in [11], which supplements the computational security of cryptography-based authentication by using PLA (i.e., information theoretical security), has an excessive signaling overhead and

would be limited for applications. In contrary, the cross-layer authentication protocols in [12–14] have limitations in terms of authentication performance, due to uncontrollable physical features in PLA. In addition, there is no theoretical analysis for the conventional cross-layer authentication protocols in terms of the authentication performance and signaling overhead. In 5G networks, both the authentication performance and signaling overhead should be considered. Consequently, it is necessary to design a sophisticated authentication protocol with a novel integration strategy to reduce network traffic in MIoT, while guaranteeing a reasonable authentication performance under poor communication environments.

3. Physical Layer Aided Authentication and Key Agreement (PL-AKA)

In this section, we present a novel authentication protocol, which integrates a PHY-CRAM scheme [8] and cryptography-based authentication (i.e., AKA) as a good candidate of cross-layer authentication protocol for MIoT systems. It is possible to employ other PLA schemes or a generalized PLA in the proposed protocol (i.e., generalization of the proposed protocol). However, it is out of scope in this paper.

3.1. Physical Layer Challenge-Response Authentication (PHY-CRAM)

In this subsection, we briefly introduce a PHY-CRAM, which utilizes channel phase information to encapsulate a secret key for authentication in multicarrier systems. The PHY-CRAM is integrated into a conventional AKA in the proposed protocol for which details will be discussed in the following Section 3.2.2. The PHY-CRAM [8] is divided into three steps: the physical layer challenge, response, and verification as follows.

3.1.1. Physical Layer Challenge

Suppose that a legitimate IoT device wants to be authenticated by a BS with a shared secret key, while an intrusion device that has no knowledge of the secret key tries implementing impersonation attacks. They use L subcarriers to communicate with each other. If the IoT device sends a request signal to the BS requesting authentication, the BS transmits a pilot signal to the IoT device to perform the channel estimation for the physical layer challenge. The challenge signal from the BS in a time domain can be represented as follows:

$$x_C(t) = \sum_{l=1}^L \sqrt{\frac{2E_s}{T}} \cos(2\pi f_l t), \quad (1)$$

where E_s and T denote the energy per symbol and the symbol duration, respectively. In addition, it is assumed that sinusoids denoted by $\cos(2\pi f_l t)$ are sufficiently separated so that the L sinusoids are all orthogonal to each other. Then, the channel phase of the received signal at the IoT device through the l th subcarrier is given by the following:

$$Y_C(f_l) = e^{j\hat{\theta}_l} |H(f_l)| X_C(f_l) + n(f_l), \quad (2)$$

where $H(f_l)$ and $n(f_l)$ are the l th channel coefficient, and noise term, respectively, which are assumed to be independent and identically distributed CSCG random variables, i.e., $H(f_l) \sim \mathcal{CN}(0, \sigma_h^2)$ (for Rayleigh fading) and $n(f_l) \sim \mathcal{CN}(0, \sigma^2)$. Then, the channel phase can be obtained as follows: $e^{j\hat{\theta}_l} = \frac{Y_C(f_l)}{|Y_C(f_l)|}$, where $\hat{\theta}_l$ is the l th estimated channel phase. The estimated channel phases are used for encapsulation of a secret key in the following physical layer response.

3.1.2. Physical Layer Response

In the physical layer response, a secret key for authentication is securely transmitted to the BS based on the estimated channel information from the challenge signal. In detail, a secret key denoted by $\kappa = [\kappa_1, \kappa_2 \cdots \kappa_L]$ is shifted by the estimated channel phases $\hat{\theta}_1, \hat{\theta}_2 \cdots \hat{\theta}_L$ to prevent the intrusion device from capturing any knowledge of the secret

key from the response signal. Note that the channel phases accounted in the proposed scheme provide more secure encryption, compared to the gain, due to their sensitivity and unpredictable nature to the locations of transceivers. Then, the transmitted signal in the physical layer response is represented as follows:

$$x_R(t) = \sum_{l=1}^L \sqrt{\frac{2E_s}{T}} \cos(2\pi f_l t + \phi_l - \hat{\theta}_l), \quad (3)$$

where $\phi_l = \frac{(1-\kappa_l)\pi}{2}$. Then, due to channel reciprocity, the received signal at the BS through the l th subcarrier is given by the following:

$$Y_R(f_l) = e^{j\tilde{\theta}_l} |H(f_l)| X_R(f_l) + n(f_l), \quad (4)$$

where $\tilde{\theta}_l = \theta_l - \hat{\theta}_l$ and $n(f_l)$ are the estimation error for the l th channel phase and noise term, respectively.

3.1.3. Physical Layer Verification

In the conventional PHY-CRAM [8], it is decided whether a received signal is transmitted from a legitimate IoT device or an intrusion device in the physical layer verification step. To this end, two hypotheses are considered: \mathcal{H}_1 is the alternative hypothesis that the received signal is transmitted by the legitimate IoT device with a legitimate secret key denoted by κ_{AB} , and \mathcal{H}_0 is the null hypothesis that the received signal is transmitted by the intrusion device with an arbitrary secret key denoted by κ_E . In [8], the test statistics of $\zeta = |\kappa_{AB} \mathbf{Y}_R^T|$ are used for binary hypothesis testing. Here, $\mathbf{Y}_R = [Y_R(f_1), Y_R(f_2), \dots, Y_R(f_L)]$ is a received vector in the response stage. In this paper, based on the test statistics of ζ , a novel cross-layer authentication strategy integrating the PHY-CRAM scheme to the cryptography-based authentication is proposed, for which details are provided in the following subsection.

3.2. Proposed PL-AKA Protocol

In this subsection, we propose a PL-AKA, which prevents severe network congestion in core networks and minimizes the computational complexity for authentication of low-cost IoT devices in MIoT systems. To this end, the notion of local security is investigated, and the PHY-CRAM [8] is applied to a conventional AKA protocol with a novel integration strategy to resist impersonation attacks from malicious intruders. A BS plays a crucial role in authenticating an IoT device through the PHY-CRAM scheme, which is employed to alleviate traffic loads in core networks in the proposed protocol. Here, the PHY-CRAM can effectively protect the attacks by preemptively detecting a forged signal at a BS. Although the extra burden of a BS arises from the preemptive authentication, it is relatively small because the PHY-CRAM using channel state information (CSI) does not require high computational complexity. On the other hand, the PHY-CRAM itself may not provide acceptable authentication performance under bad communication environments (e.g., low SNR), whereas it enables fast authentication with low complexity. Therefore, it is crucial to design a novel integration strategy, which exploits advantages of both the PHY-CRAM and cryptography-based authentication.

3.2.1. Integration Strategy

In the conventional PHY-CRAM [8], a certain threshold is applied to the binary hypothesis testing for authentication decision. Then, the BS may make a wrong authentication decision with the test statistics of ζ , due to noise and interference. Therefore, a core of the integration strategy is how to define a statistical range that is prone to the preemptive authentication failure. To this end, the preemptive authentication result in the proposed protocol is divided into three cases: “Black”, “Gray” and “White”, instead of a binary decision for conventional PLA as to whether the received signal is legitimate or

not. In “Black” and “White”, the BS can be sure about whether the received signal is from an intruder or from a legitimate IoT device, respectively, with high probability. On the other hand, in “Gray”, the BS is not sure about whether or not the signal is a legitimate one. Therefore, in the proposed protocol, we stipulate that “Gray” is an ambiguous result about which it is hard to make a firm decision in the physical layer, and put off the final decision to the upper layer cryptography-based authentication. Note that the result in the PHY-CRAM method is determined in accordance with test statistic ζ . Then, to determine a preemptive result in the PHY-CRAM method, two thresholds denoted by α_0 and α_1 are used in the physical layer verification, while a conventional PLA method uses a threshold to make a decision between “Black” and “White”. Thus, if the preemptive result is “White” or “Black”, the authentication is complete (i.e., cryptography-based authentication is not performed). On the other hand, if the result is “Gray”, cryptography-based authentication is performed to make a final authentication decision at the MME.

3.2.2. Procedures of Proposed Protocol

Based on the integration strategy, detailed procedures of the proposed PL-AKA [17] are illustrated in Figure 1. As shown in the chart, ten messages, which are divided in three steps—(i) initial attach ($M_1 \sim M_2$), (ii) key generation and distribution ($M_3 \sim M_4$), and (iii) authentication ($M_5 \sim M_{10}$)—are exchanged as follows:

- M_1 : The IoT device sends international mobile subscriber identity (IMSI) from the universal subscriber identity module (USIM) card of the device for user identification.
- M_2 : The MME requests authentication data to the HSS by forwarding user identification and network information.
- M_3 : The HSS generates authentication vectors (AVs) which include a secret key for PLA and transmits them to the MME.
- M_4 : The MME forwards the secret key for the PHY-CRAM to the BS, while it retains the other authentication information used for cryptographic challenge–response authentication.
- M_5 : For authentication of the IoT device, the BS transmits a challenge signal to the IoT device.
- M_6 : The IoT device sends the BS a response signal with a secret key which is encapsulated with channel phases.
- M_7 : For authentication of the network, the IoT device transmits a challenge signal to the BS.
- M_8 : The BS sends the IoT device a response signal with a secret key, which is encapsulated with channel phases.
- M_9 : If a feature score is in “Gray”, the MME selects an unused AV, retrieves RAND and AUTN, and sends them to the IoT device. Here, RAND and AUTN mean random challenge and authentication token, respectively, in cryptography-based authentication.
- M_{10} : If a feature score is in “Gray”, the IoT device authenticates the networks and transmits RES to the MME. Here, RES means response in cryptography-based authentication.

The main difference between the proposed protocol and an existing AKA protocol (e.g., EPS-AKA) is that the PHY-CRAM scheme comes under the authentication step, whereas the steps of (i) the initial attach and (ii) the key generation and distribution steps are similar to those of the conventional AKA protocol. At this time, an important issue that arises is how to integrate PLA with cryptography-based authentication. To this end, as shown in Figure 1, the PHY-CRAM method is employed as preemptive authentication between the IoT device and the BS. After performing the PHY-CRAM method, it is determined whether to conduct cryptography-based authentication procedures (M_9 and M_{10}) in the protocol in accordance with a result of the preemptive authentication.

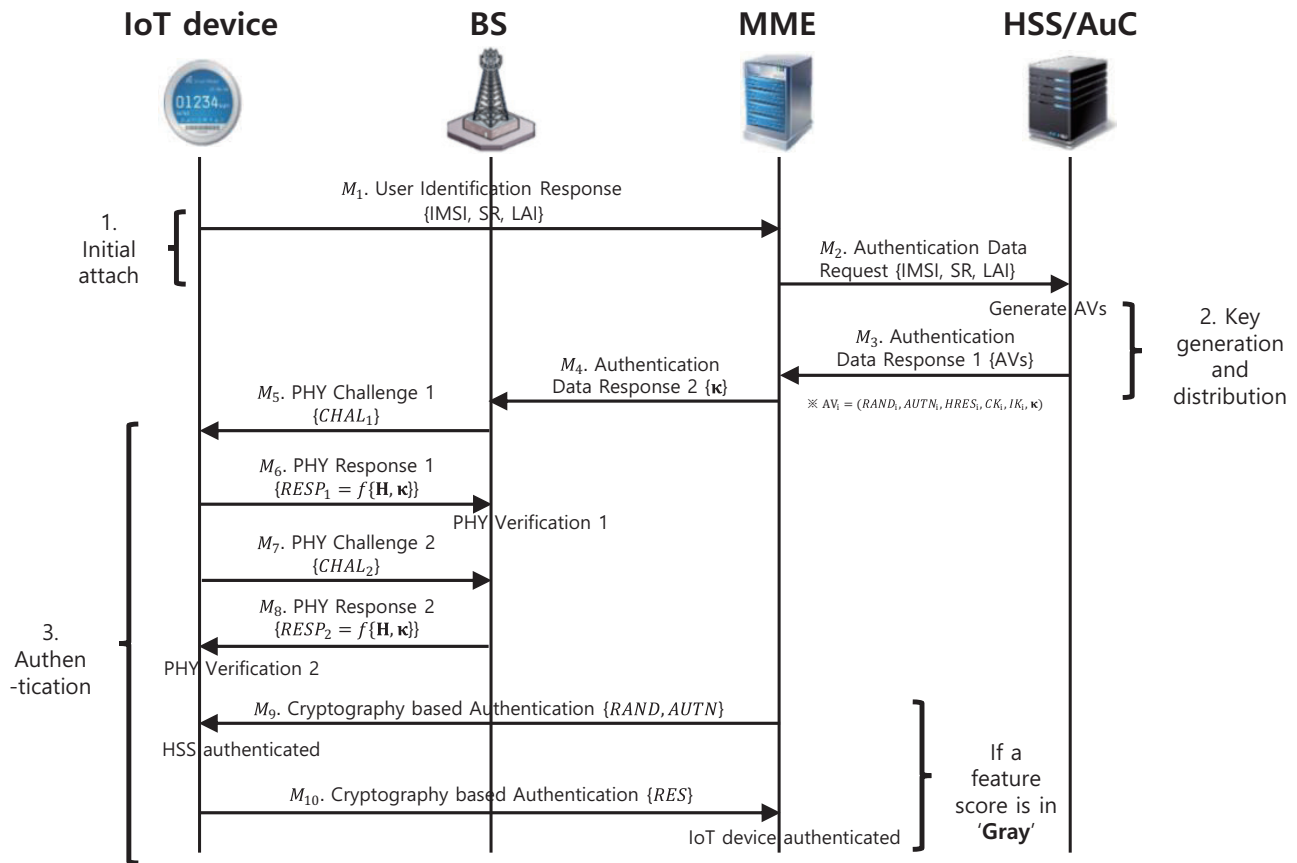


Figure 1. PL-AKA cross-layer authentication protocol [17].

4. Performance Analysis

In this section, the proposed PL-AKA is theoretically analyzed in terms of the authentication error probability and signaling overhead under a MIoT system scenario. In addition, an experiment using USRP is performed to demonstrate the benefits of integrating PLA with an AKA protocol.

4.1. Theoretical Analysis

To evaluate the proposed authentication scheme, we consider an authentication error probability, which is an incorrect decision probability at the BS and given by the following:

$$P_E = \rho P_M + (1 - \rho) P_F \quad (5)$$

where P_M and P_F are the miss and false alarm probabilities at the BS, respectively, and ρ is a weighting factor ($0 \leq \rho \leq 1$). Note that $P_E = 0$ is assumed in the conventional cryptography-based authentication. P_M is the probability that when the legitimate IoT device transmits, the BS decides that the signal is an intrusion signal; P_F is the probability that when the intrusion device transmits, the BS decides that the signal is a legitimate signal. As shown in [8], the distribution of $f_{\zeta|\mathcal{H}_i}(x)$ is the Rice distribution as follows:

$$f_{\zeta|\mathcal{H}_i}(x) = \frac{x}{\sigma_i^2} e^{-\frac{x^2 + v_i^2}{2\sigma_i^2}} I_0\left(\frac{xv_i}{\sigma_i^2}\right), \quad x \geq 0 \quad \text{and} \quad i = 0, 1 \quad (6)$$

$$F_{\zeta|\mathcal{H}_i}(x) = 1 - \mathcal{Q}_1\left(\frac{v_i}{\sigma_i}, \frac{x}{\sigma_i}\right) \quad (7)$$

where $\nu_i = \mathbb{E}[\zeta|\mathcal{H}_i]$, $\sigma_i^2 = \text{Var}[\zeta|\mathcal{H}_i]$ and $\mathcal{Q}_1(x, y)$ is the Marcum Q-function respectively [18]. For given target miss and false alarm probabilities denoted by P_M° and P_F° , respectively, the thresholds are determined as follows:

$$\alpha_1 = \underset{\alpha}{\operatorname{argmax}} F_{\zeta|\mathcal{H}_1}(\alpha) \leq P_M^\circ \quad (8)$$

$$\alpha_0 = \underset{\alpha}{\operatorname{argmax}} (1 - F_{\zeta|\mathcal{H}_0}(\alpha)) \leq P_F^\circ \quad (9)$$

Then, based on the target miss and false alarm probabilities, the authentication error probability can be obtained in the proposed protocol—that is, we can control the authentication performance with P_M° and P_F° . However, it should be noted that if P_M° and P_F° are too low, it can induce a large signaling overhead. We compare the proposed protocol with the conventional EPS-AKA protocol in terms of the signaling overhead. As mentioned in the previous subsection, the thresholds (α_1 and α_0) are determined with P_M° and P_F° , respectively. Then, the ranges of the three cases (i.e., “Black”, “Gray” and “White”) are determined as follows:

$$\Theta = \begin{cases} \text{White} & \text{if } \zeta > \alpha_0 \\ \text{Gray} & \text{if } \alpha_1 \leq \zeta \leq \alpha_0 \\ \text{Black} & \text{if } \zeta < \alpha_1 \end{cases} \quad (10)$$

Note that the lower the target miss and false alarm probabilities are set, the larger the distance between α_1 and α_0 , which determines the range that “Gray” becomes. Let λ denote the probability of “Gray” (i.e., $p(\alpha_1 \leq \zeta \leq \alpha_0)$). Thus, the probability is given by the following:

$$\lambda = \rho(F_{\zeta|\mathcal{H}_1}(\alpha_0) - F_{\zeta|\mathcal{H}_1}(\alpha_1)) + (1 - \rho)(F_{\zeta|\mathcal{H}_0}(\alpha_0) - F_{\zeta|\mathcal{H}_0}(\alpha_1)) \quad (11)$$

From [19] and Table 1, the signaling overheads of EPS-AKA and PHY-PCRAS-AKA [11] are given as follows:

$$\Omega_{\text{EPS-AKA}} = N(704 + 608U + 528(P - 1)), \quad (12)$$

$$\Omega_{\text{PHY-PCRAS-AKA}} = N\left(\sum_{m=1}^{10} |M_m|\right) + N(P - 1)(|M_1| + \sum_{q=5}^{10} |M_q|) \quad (13)$$

$$\Omega_{\text{PHY-PCRAS-AKA}_{\text{MME}}} = N\left(\sum_{m=1}^4 |M_m| + \sum_{n=9}^{10} |M_n|\right) + N(P - 1)(|M_1| + \sum_{q=9}^{10} |M_q|) \quad (14)$$

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 Figure 1, the M_9 and the M_{10} messages associated with the cryptography-based authentication are exchanged with a probability of $\tilde{\lambda} = 1 - (1 - \lambda)^2$ for the mutual authentication. Then, the average signaling overhead of the proposed protocol and signaling overhead at MME are given by the following:

$$\mathbb{E}[\Omega_{\text{PL-AKA}}] = N\left(\sum_{m=1}^8 |M_m| + \tilde{\lambda} \sum_{n=9}^{10} |M_n|\right) + N(P - 1)(|M_1| + \sum_{p=5}^8 |M_p| + \tilde{\lambda} \sum_{q=9}^{10} |M_q|) \quad (15)$$

$$\mathbb{E}[\Omega_{\text{PL-AKA}_{\text{MME}}}] = N\left(\sum_{m=1}^4 |M_m| + \tilde{\lambda} \sum_{n=9}^{10} |M_n|\right) + N(P - 1)(|M_1| + \tilde{\lambda} \sum_{q=9}^{10} |M_q|) \quad (16)$$

where M_i is the i th message in the proposed protocol. Based on the related parameters in Table 1, $|M_1| = |M_2| = 176$, $|M_3| = 608U + L$, $|M_4| = |M_5| = |M_6| = |M_7| = |M_8| = L$, $|M_9| = 288$, and $|M_{10}| = 64$. The signaling overhead of the PL-AKA depends on L and λ determined by P_M° and P_F° .

Table 1. Related 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
RAND	Random challenge	128
AUTN	Authentication token	160
κ	Secret key for PHY-CRAM	L
AV	Authentication vector	$608 + L$

We present the simulation results to see the authentication and signaling overhead performance of the proposed protocol. For simulations, we assume the Rayleigh fading channel model and generate random phases, where $H(f_l) \sim \mathcal{CN}(0, \sigma_h^2)$ and define SNR as $10\log_{10}(\frac{E_s}{\sigma^2})$.

Figure 2 depicts the probability density functions of ζ for legitimate and intrusion signals in which $P_M^\circ = P_F^\circ = 10^{-6}$, $L = 64$, and SNR = 5 dB. As shown in Figure 2, the distribution of $\zeta|\mathcal{H}_1$ from the legitimate device is sufficiently distinguishable from that of $\zeta|\mathcal{H}_0$, the intrusion one. In addition, the ranges of the three cases (“Black”, “Gray” and “White”) are determined by two thresholds (α_1 and α_0) with P_M° and P_F° . Here, “Gray” plays a role as a guard interval to prevent a wrong authentication decision of a BS caused by noise and interference. From Figure 2, it seems obvious that the probability that ζ is included in “Gray” is negligibly low, compared to “Black” and “White”. It implies that the signaling overhead induced by cryptography-based authentication (i.e., M_9 and M_{10}) is insignificant. Figure 3 shows the simulation results for the signaling overhead over different target false alarm probabilities to compare the proposed PL-AKA with conventional EPS-AKA and physical layer phase challenge response authentication AKA (PHY-PCRAS-AKA) [11], where $L = 64$, $P = 30$, $U = 20$, $N = 200$, $P_M^\circ = 10^{-6}$ and SNR = 5 dB. In the simulation, the signaling overhead is divided into two types: (i) total signaling overhead, and (ii) signaling overhead at MME. As shown in Figure 3, although $P_M^\circ = 10^{-10}$, the proposed PL-AKA has a small total signaling overhead, compared to the conventional methods. In particular, the PHY-PCRAS-AKA needs a larger signaling overhead than EPS-AKA because it simply cascades both layer authentication methods for the enhancement of security as described in (13) and (14). Furthermore, while the signaling overhead at MME is the same as the total signaling overhead in the conventional EPS-AKA, in the proposed PL-AKA, the signaling overhead at MME is significantly smaller than the total signaling overhead because the BS performs a preemptive authentication instead of the MME in the proposed PL-AKA protocol.

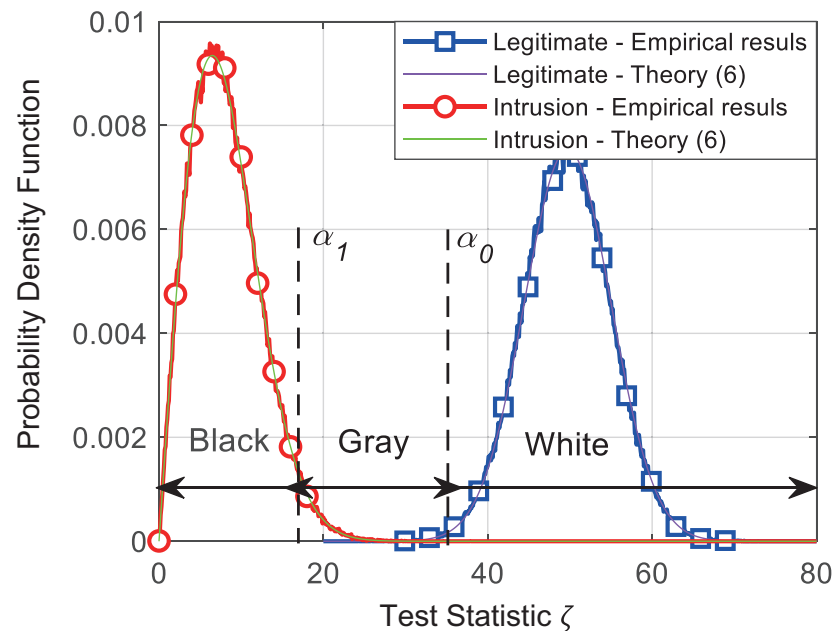


Figure 2. Comparison of the probability density functions.

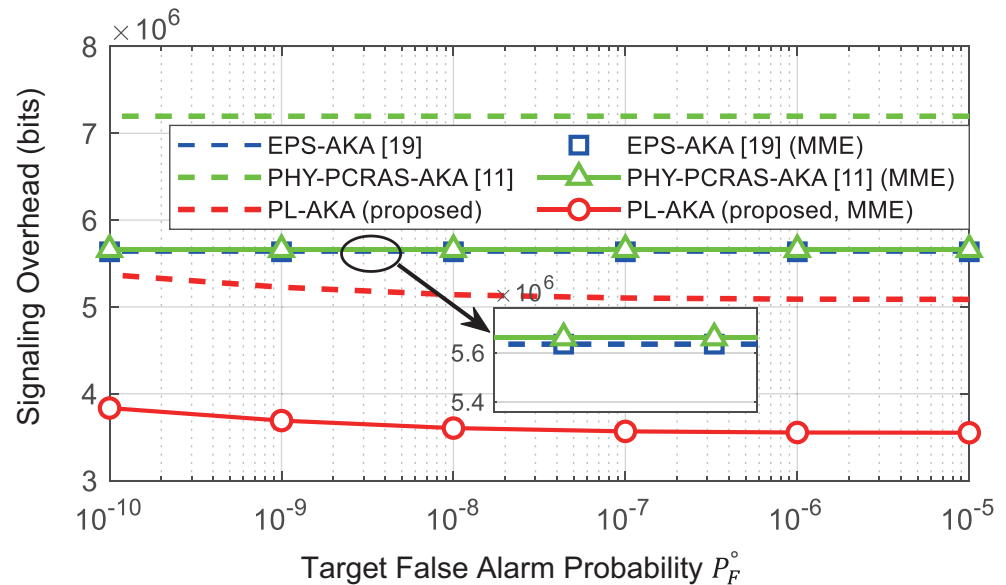


Figure 3. Signaling overheads of PL-AKA and EPS-AKA over various target false alarm probabilities (simulation results).

4.2. Experiment Analysis

In this subsection, we implement an experiment to demonstrate the practical performance of the proposed PL-AKA. To this end, a USRP based test-bed is designed in an LTE communication environment. In the experiment, phase sanitization introduced in [20] is employed to compensate for the effect of the carrier frequency offset (CFO) and sampling timing offset (STO) for channel reciprocity. Figure 4 shows the reciprocity of sanitized channel phase ($\hat{\theta}$) in our preliminary test [21]. From this result, we simply suppose that a BS transmits the challenge signal to a user equipment (UE) for PHY-CRAM. For the performance test of PL-AKA, the test statistics are defined and the probability of “Gray” (i.e., λ) is calculated to compare the signaling overhead with the conventional scheme.

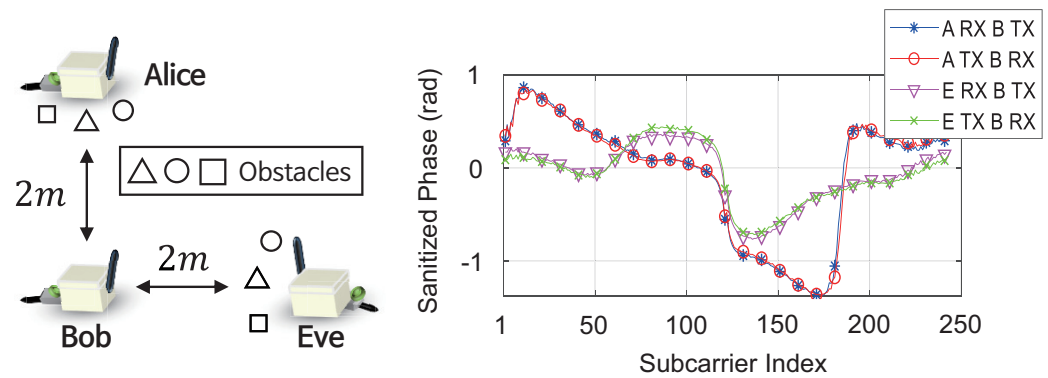


Figure 4. Preliminary test for verifying channel reciprocity of sanitized phase [21].

Experiment Setup

Figure 5 illustrates the experimental environment. The experiment is designed with 2 NI-USRP 2944R [22] and LTE application framework 2.0 [23] running on Labview NXG 4.0 [24] of National Instrument. The host-PC is Dell Inspiron 3650 [25] with Intel Core i5, and having 16 GB of RAM. Each USRP is connected to PCI express port of the PC and one USRP is served as a BS, and the other is served as an UE. To measure CSI according to a physical location, the UE is settled onto i-ROBO PSA-125-S motion stage [26] with Autronics PMC-1HS-USB controller [27]. UE moves 50 locations that are 2 cm apart from each other, measuring the 1000 CSI frames in each location. In the given situation, BS and UE are remotely controlled by a laptop to avoid channel distortion and maintain the channel coherence time as long as possible. The experiment is operated for 10 h. Tables 2 and 3 indicate the USRP specifications and communication parameters, respectively.

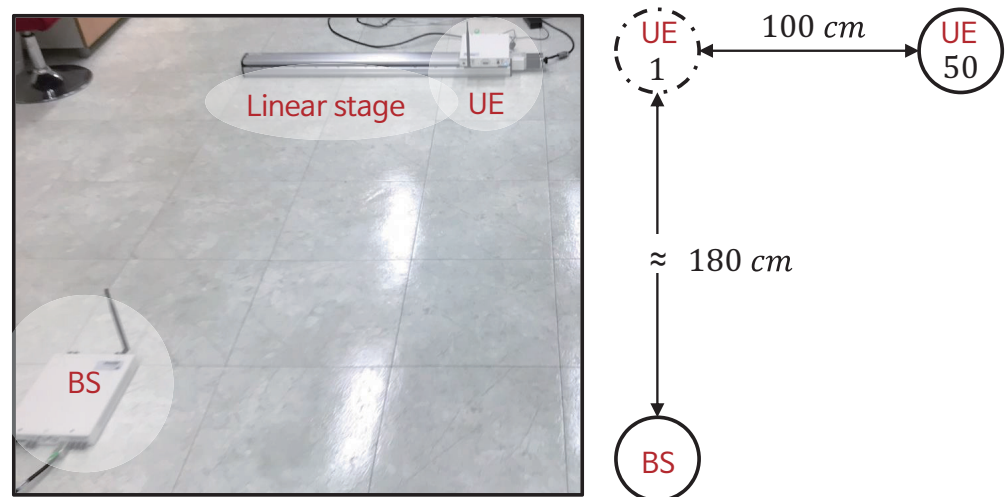


Figure 5. Experiment setup for measuring physical channels.

Table 2. USRP 2944R specifications [22].

Transmitter	
Frequency range	10 MHz to 6 GHz
Frequency step	<1 kHz
Maximum output power (P_{out})	17 dBm to 20 dBm
Gain range	0 dB to 31.5 dB
Gain step	0.5 dB
Frequency accuracy	2.5 ppm
Maximum instantaneous real-time bandwidth	160 MHz
Maximum I/Q sample rate	200 MS/s
Digital to analog converter resolution and dynamic range	16 bit, 80 dB
Receiver	
Frequency range	10 MHz to 6 GHz
Frequency step	<1 kHz
Gain range	0 dB to 37.5 dB
Gain step	0.5 dB
Frequency accuracy	2.5 ppm
Maximum input power (P_{in})	−15 dBm
Noise figure	5 dB to 7 dB
Maximum instantaneous real-time bandwidth	160 MHz
Maximum I/Q sample rate	200 MS/s
Digital to analog converter resolution and dynamic range	14 bit, 88 dB

Table 3. Software defined communication conditions.

Communication Parameters	
Center carrier frequency	1.0 GHz
Wavelength	30 cm
Bandwidth	20 MHz
Modulation	QPSK (MCS 0)
The # of subcarrier	1200
The # of channel estimation	200
Channel estimation subcarrier	Cell reference signal (CRS)

4.3. Root Mean Square Distance (RMSD) Test Statistic

Utilizing the sanitized phase, RMSD can also be a simple alternative test statistic instead of [8]. Let us denote RMSD as η , which is defined with the following equation:

$$\eta_k^{(L_i, L_j)} = \text{RMSD}(\bar{\theta}_{Ref}^{(L_i)}, \bar{\theta}_k^{(L_j)}) = \sqrt{\frac{\sum_{r=1}^n \left(\bar{\theta}_{Ref, r}^{(L_i)} - \bar{\theta}_{k, r}^{(L_j)} \right)^2}{n}} \quad (17)$$

where k and r are k th estimated frame and r th subcarrier of the frame, n is the number of subcarrier and L_i and L_j are the i th and j th location indices, respectively. Here, channel estimation of the 1st frame from a location i is selected for the reference frame $\bar{\theta}_{Ref}^{(L_i)}$.

4.4. Effect of Spatial Correlation

In general, an eavesdropper in the vicinity of a legitimate receiver may obtain a legitimate CSI by exploiting spatial correlation. Thus, a measured RMSD within a half-wavelength distance from i th location is not regarded in order to simplify the analysis.

4.5. Effect of Inter-carrier Dependency

Another constraint that arises in measuring test statistics is inter-carrier dependency. Figure 6 describes two different channels: simulated Rayleigh independent fading channel, and measured channel from the experiment. In this situation, (a) can extract useful information as the number of subcarrier increases, but (b) provides no additional information, even if it exploits the entire CRS subcarrier to encapsulate the secret key. This result implies that however a number of subcarriers are used, there is no significant reliability increase, but it improves the secrecy ability with the extension of the key length. From the point of view of reliability and computational efficiency, the selective subcarrier benefits from the signaling overhead, but it has to sacrifice its secrecy ability.

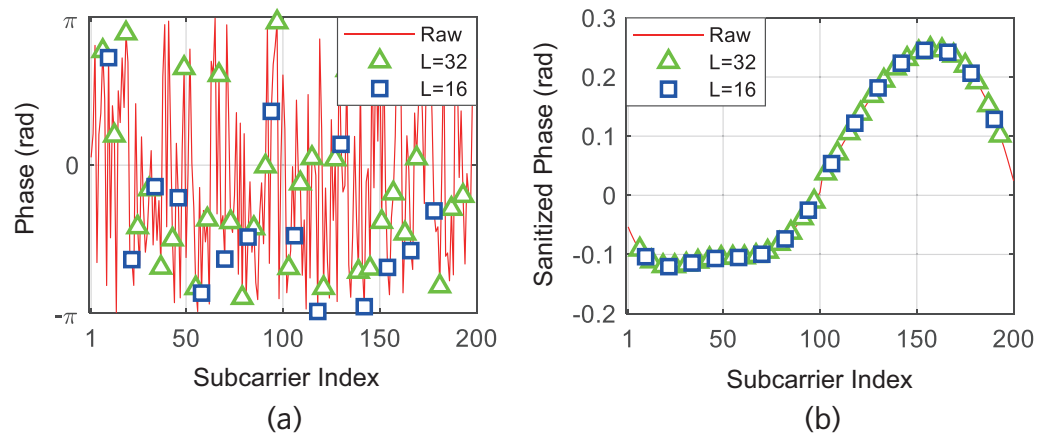


Figure 6. Raw and irregularly sampled channel phase profiles of (a) independently simulated and (b) USRP experimented correlated channels.

4.6. Experimental Results

Figure 7 is the histogram of the RMSD results of the experiment. For ease of comprehension, we assume that the profiles can be fitted as a log-normal distribution, i.e., $\ln(X) \sim (\nu_i, \sigma_i^2)$ that PDF and CDF are defined by the following:

$$f_{\eta|\mathcal{H}_i}(x) = \frac{1}{x\sigma_i\sqrt{2\pi}} e^{-\frac{(\ln x - \nu_i)^2}{2\sigma_i^2}}, \quad x > 0 \quad \text{and} \quad i = 0, 1 \quad (18)$$

$$F_{\eta|\mathcal{H}_i}(x) = \frac{1}{2} + \frac{1}{2} \operatorname{erf}\left(\frac{\ln x - \nu_i}{\sqrt{2}\sigma_i}\right) \quad (19)$$

where $\nu_i = \mathbb{E}[\eta|\mathcal{H}_i]$, $\sigma_i^2 = \operatorname{Var}[\eta|\mathcal{H}_i]$ and $\operatorname{erf}(x)$ is error function [28] respectively. From the above equations, P_M° , P_F° and λ can be induced by applying the concept in Equations (8)–(10), conversely. Then, in the case of RMSD, the thresholds are determined as follows:

$$\alpha_1 = \operatorname{argmax}_{\alpha} (1 - F_{\eta|\mathcal{H}_1}(\alpha)) \leq P_M^\circ \quad (20)$$

$$\alpha_0 = \operatorname{argmax}_{\alpha} F_{\eta|\mathcal{H}_0}(\alpha) \leq P_F^\circ \quad (21)$$

As shown in Figure 8, “Black”, “Gray” and “White” are determined as follows:

$$\Theta = \begin{cases} \text{Black} & \text{if } \eta > \alpha_1 \\ \text{Gray} & \text{if } \alpha_0 \leq \eta \leq \alpha_1 \\ \text{White} & \text{if } \eta < \alpha_0 \end{cases} \quad (22)$$

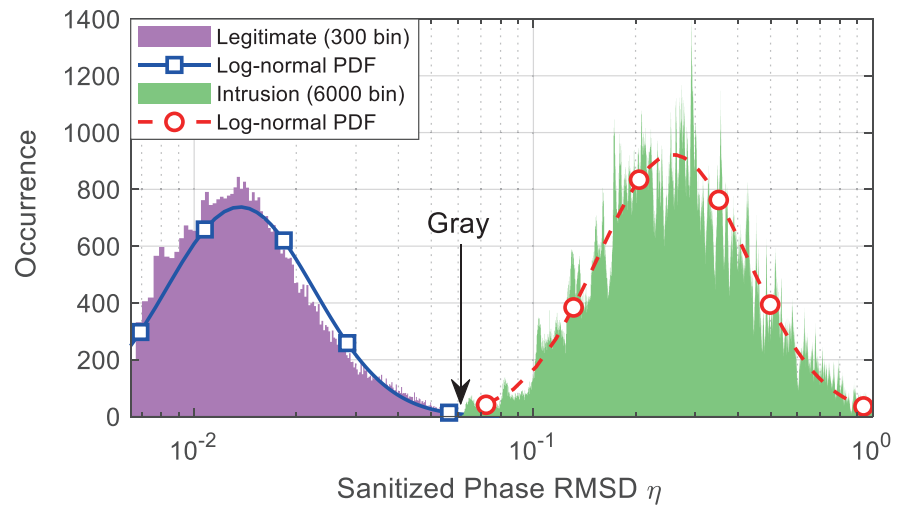


Figure 7. Histogram of sanitized phase RMSD η .

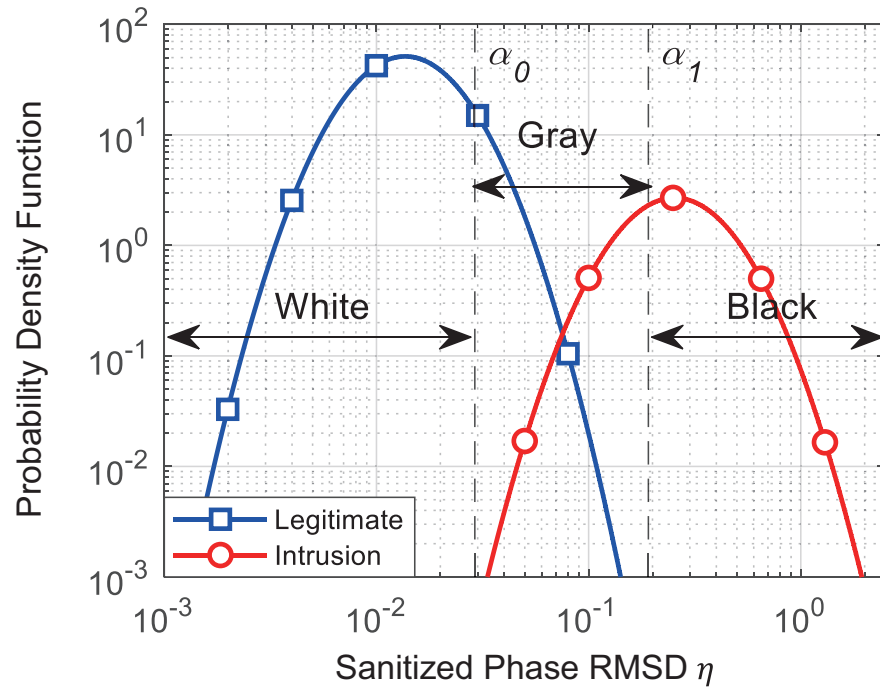


Figure 8. PDFs of RMSD for PL-AKA.

Figure 9 shows that the signaling overhead of conventional EPS-AKA and the proposed PL-AKA in different numbers of subcarriers and target false alarm rates, where $P = 30$, $U = 20$, $N = 200$, $P_M^o = 10^{-6}$. In addition, we investigated not only the signaling overhead of total protocol, but also that of MME as described in (16). In terms of entire protocol, it alleviates the burden of MME, which can be desirable for the future in distributed networks. In addition, the proposed scheme achieves a computational predominance by sacrificing the target false alarm rate. Thus, the number of subcarrier and false alarms and the miss detection probability should be coordinated moderately as its application.

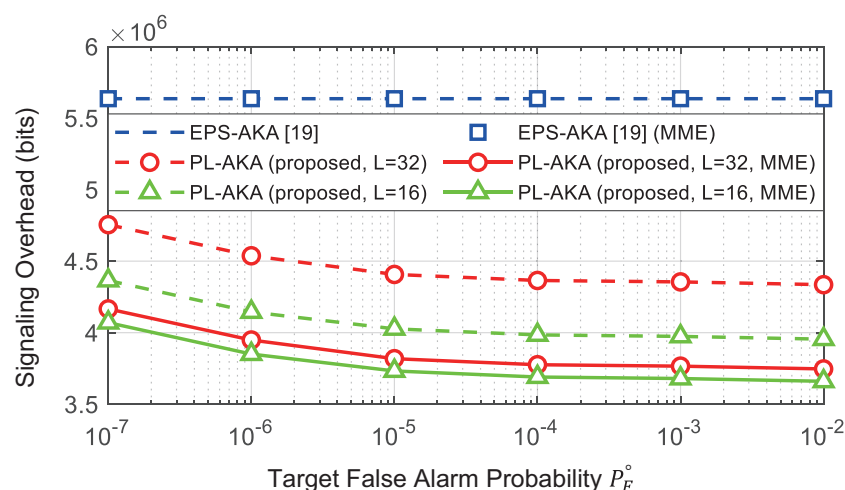


Figure 9. Signaling overheads of PL-AKA and EPS-AKA over various target false alarm probabilities (experiment results).

5. Conclusions

In this paper, we presented a lightweight PL-AKA protocol by applying PLA to conventional AKA protocol, preemptively. To this end, we considered the integration strategy of the PLA and conventional cryptography-based authentication, classifying the PLA results into three parts: “Authenticated”, “Rejected” and “Gray”. We derived the signaling overhead of the proposed PL-AKA protocol with a probability that the cryptography-based authentication is performed. Moreover, a USRP-based experimental analysis was conducted to demonstrate the proposed scheme in practical application for IoT. In this analysis, we installed BS and UE as the LTE communication system, and observed the CSI according to the physical location with the linear stage. Here, phase sanitization was introduced to neutralize the effect of CFO and STO, and RMSD was defined to separate the legitimate and intrusion channel. The proposed scheme can achieve a more efficient signaling overhead, compared to conventional schemes, in both the simulation and experimental results. Therefore, this study showed the feasibility of the proposed scheme; various approaches to reduce the “Gray” probability can be the basis of future work to further reduce authentication overheads.

Author Contributions: S.H. contributed toward the experimental analysis and data measurement. Y.L. helped in writing the introduction, investigation, resource, theoretical algorithms, review and editing, methodology. J.C. helped in the conceptualization, methodology, experimental analysis, validation, review and editing. E.H. aided in the proofreading, conceptualization, methodology, formal analysis, review and editing as the corresponding author, and provided guidance throughout the whole preparation of the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2017-0-00413, Streamlined Secure Communications by Physical Layer Identification in Cellular IoT) and this work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (2021R1A2C1009803).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are available on request due to restrictions (privacy or ethical). The data presented in this study are available on request from the corresponding author. The data are not publicly available because this data set will be used for future works.

Acknowledgments: This research was supported by Institute for Information and Communications Technology Promotion (IITP) funded by the Korea Government through the Ministry of Science

and Information and Communication Technology (MSIT) (Streamlined Secure Communications by Physical Layer Identification in Cellular IoT) under Grant 2017-0-00413, and this work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (2021R1A2C1009803).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

5G	Fifth-generation
USRP	Universal software radio peripheral
IoT	Internet of Things
MIoT	Massive internet of things
AKA	Authentication and key agreement
EPS-AKA	Evolved packet system AKA
PLA	Physical layer authentication
PHY-CRAM	Physical layer challenge-response authentication mechanism
PL-AKA	Physical layer aided AKA
CSCG	Circularly symmetric complex Gaussian
MME	Mobility management entity
CFO	Carrier frequency offset
STO	Sampling timing offset
BS	Base station
UE	User equipment
IMT	International mobile telecommunication
HSS	Home subscriber server
RANs	Radio access networks
SNR	Signal-to-noise ratio
CSI	Channel state information

References

1. Samsung, Republic of Korea. The Next Hyper Connected Experience for All. Available online: <https://research.samsung.com/next-generation-communications> (accessed on 29 June 2021).
2. Abdrabou, M.A.; Elbayoumy, A.D.E.; Abd El-Wanis, E. LTE authentication protocol (EPS-AKA) weaknesses solution. In Proceedings of the 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS), IEEE, Cairo, Egypt, 12–14 December 2015; pp. 434–441.
3. Kumar, P.; Gurtov, A.; Sain, M.; Martin, A.; Ha, P.H. Lightweight authentication and key agreement for smart metering in smart energy networks. *IEEE Trans. Smart Grid* **2018**, *10*, 4349–4359. [\[CrossRef\]](#)
4. Modiri, M.M.; Mohajeri, J.; Salmasizadeh, M. GSL-AKA: Group-based secure lightweight authentication and key agreement protocol for M2M communication. In Proceedings of the 2018 9th International Symposium on Telecommunications (IST), IEEE, Tehran, Iran, 17–19 December 2018; pp. 275–280.
5. Li, J.; Wen, M.; Zhang, T. Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks. *IEEE Internet Things J.* **2015**, *3*, 408–417. [\[CrossRef\]](#)
6. Liu, Y.; Chen, H.H.; Wang, L. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 347–376. [\[CrossRef\]](#)
7. Lee, Y.; Hwang, E.; Choi, J. A unified approach for compression and authentication of smart meter reading in AMI. *IEEE Access* **2019**, *7*, 34383–34394. [\[CrossRef\]](#)
8. Wu, X.; Yang, Z. Physical-layer authentication for multi-carrier transmission. *IEEE Commun. Lett.* **2014**, *19*, 74–77. [\[CrossRef\]](#)
9. Wu, X.; Yang, Z.; Ling, C.; Xia, X.G. Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission. *IEEE Trans. Commun.* **2016**, *15*, 6611–6625. [\[CrossRef\]](#)
10. Shan, D.; Zeng, K.; Xiang, W.; Richardson, P.; Dong, Y. PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1817–1827. [\[CrossRef\]](#)
11. Wu, X.; Yang, Z.; Ling, C.; Xia, X.G. A physical-layer authentication assisted scheme for enhancing 3GPP authentication. *arXiv* **2015**, arXiv:1502.07565.
12. Wen, H.; Wang, Y.; Zhu, X.; Li, J.; Zhou, L. Physical layer assist authentication technique for smart meter system. *IET Commun.* **2013**, *7*, 189–197. [\[CrossRef\]](#)
13. Moreira, C.M.; Kaddoum, G.; Bou-Harb, E. Cross-layer authentication protocol design for ultra-dense 5G HetNets. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), IEEE, Kansas City, MO, USA, 20–24 May 2018; pp. 1–7.

14. Abdelaziz, A.; Koksai, C.E.; Burton, R.; Barickman, F.; Martin, J.; Weston, J.; Woodruff, K. Beyond PKI: Enhanced authentication in vehicular networks via MIMO. In Proceedings of the 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), IEEE, Kalamata, Greece, 25–28 June 2018; pp. 1–5.
15. Marcus, M.J. 5G and “IMT for 2020 and beyond” [Spectrum Policy and Regulatory Issues]. *IEEE Wirel. Commun.* **2015**, *22*, 2–3. [CrossRef]
16. Cao, J.; Ma, M.; Li, H. LPPA: Lightweight privacy-preservation access authentication scheme for massive devices in fifth Generation (5G) cellular networks. *Int. J. Commun. Syst.* **2019**, *32*, e3860. [CrossRef]
17. Lee, Y.; Hwang, E.; Choi, J. Physical layer aided authentication and key agreement for the Internet of Things. In Proceedings of the 2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS), IEEE, Virtual, 14–16 December 2020; pp. 1–7.
18. Nutall, A.H. Some integrals involving the QM function. *IEEE Trans. Inf. Theory* **1975**, *21*, 95–96. [CrossRef]
19. Lai, C.; Li, H.; Li, X.; Cao, J. A novel group access authentication and key agreement protocol for machine-type communication. *Trans. Emerg. Telecommun. Technol.* **2015**, *26*, 414–431. [CrossRef]
20. Qian, K.; Wu, C.; Yang, Z.; Liu, Y.; Zhou, Z. PADS: Passive detection of moving targets with dynamic speed using PHY layer information. In Proceedings of the 2014 20th IEEE international conference on parallel and distributed systems (ICPADS), IEEE, Hsinchu, Taiwan, 16–19 December 2014; pp. 1–8.
21. Han, S.; Lee, Y.; Hwang, E. Experimental analysis on secret key generation scheme based on wireless channel state information using USRP. *Korean Inst. Comms Info. Sci. (KICS)* **2019**, 302–303.
22. National Instrument Corporation, United of States. USRP-2944 Specifications. Available online: <https://www.ni.com/pdf/manuals/375724b.pdf> (accessed on 12 July 2021).
23. National Instrument Corporation, United of States. LabVIEW Communications LTE Application Framework 2.0 and 2.0.1. Available online: <https://www.ni.com/ko-kr/support/documentation/supplemental/16/labview-communications-lte-application-framework-2-0-and-2-0-1.html> (accessed on 12 July 2021).
24. National Instrument Corporation, United of States. LabVIEW NXG 4.0 Readme. Available online: <https://www.ni.com/pdf/manuals/376808g> (accessed on 12 July 2021).
25. Dell Technologies, United of States. Inspiron 3650 specifications. Available online: https://downloads.dell.com/manuals/all-products/esuprt_desktop/esuprt_inspiron_desktop/inspiron-3650-desktop_reference%20guide_en-us.pdf (accessed on 12 July 2021).
26. i-ROBO, Republic of Korea. PSA-125-S. Available online: http://www.i-robo.kr/en/bbs/board.php?bo_table=2_2_en (accessed on 12 July 2021).
27. Autonics, Republic of Korea. PMC-1HS-USB. Available online: https://autonics.su/files/PMC_1HS_2HS_EN_MA_180822_W.pdf (accessed on 12 July 2021).
28. Chang, S.H.; Cosman, P.C.; Milstein, L.B. Chernoff-type bounds for the Gaussian error function. *IEEE Trans. Commun.* **2011**, *59*, 2939–2944. [CrossRef]