Article

Light-weight Physical Layer Aided Key Agreement and Authentication for the Internet of Things

Seungnam Han[1], Yonggu Lee[2], Jinho Choi[3], Euiseok Hwang[1,*]

[1] School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology (GIST), Gwangju 61005, South Korea; snhan0911@gm.gist.ac.kr;
[2] Security Research and Development Team, Korea Atomic Energy Research Institute (KAERI), Daejeon 34057, South Korea; ygl@kaeri.re.kr;
[3] School of Information Technology, Deakin University, Geelong, VIC 3220, Australia; jinho.choi@deakin.edu.au;
* Correspondence: euiseokh@gist.ac.kr;

† This paper is an extended version of our paper published in This article is an extended and improved 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). Conventional evolved packet system AKA (EPS-AKA) used in long-term evolution (LTE) systems may suffer from congestions in core networks by the large signaling overhead as the number of IoT devices increases. Thus, in order to alleviate the overhead, we consider a 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 signaling overhead compared to the conventional EPS-AKA in both 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

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 simultaneous authentication and susceptibility to identified attacks. Instead, physical layer authentication (PLA) has been studied for 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 the eavesdropper from impersonating- based attacks. However, PLA is inherently

Citation: Han, S.; Lee, Y.; Choi, J.; Hwang, E. Title. *Preprints* **2021**, *1*, 0. https://doi.org/

Received:
Accepted:
Published:

 doi:10.20944/preprints202107.0013.v1

difficult to guarantee authentication performance in poor communication environment. 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 signal overhead and reliability by selectively applying conventional cryptography-based authentication along with PLA and preliminary PLA decisions. To demonstrate effectiveness of the proposed protocol, 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 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 an authentication error probability and signaling overhead of the proposed protocol.

- For the validation of PLA in the proposed protocol, RF experiment is conducted with USRP transceivers.

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 (CSCG) random variable with mean μ and variance σ^2.

2. Motivation and local security

In 5G networks, supporting the high concurrent connections of a lot of 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]. 5G should cover densely populated areas such as residential buildings or business centers in urban environment [16], where large signaling overhead induced by conventional cryptographic authentication mechanisms may cause inevitable delays. Furthermore, when massive devices access to 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 traffics 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), correlated channels). Thus, cross-layer authentication protocol which integrates PLA in RANs and cryptography-based authentication in core networks is considered. However, conventional cross-layer authentication protocols [11–14] cannot provide both a reliable authentication performance and small signaling overhead for 5G networks. For example, as mentioned earlier, the authentication protocol in [11] which supplements computational security of cryptography-based authentication by using PLA (i.e., information theoretical security) has 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

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

in PLA. In addition, there is no theoretical analysis for the conventional cross-layer authentication protocols in terms of authentication performance and signaling overhead. In 5G networks, both 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 traffics 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 to a conventional AKA in the proposed protocol of which details will be discussed in the following subsection 3.2.2. The PHY-CRAM [8] is divided into three steps: 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 which has no knowledge for the secret key tries 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:

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

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 enough 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

$$Y_C(f_l) = e^{j\theta_l} |\mathrm{H}(f_l)| X_C(f_l) + \mathrm{n}(f_l), \tag{2}$$

where $\mathrm{H}(f_l)$ and $\mathrm{n}(f_l)$ are the l^{th} channel coefficient, and noise term, respectively, which are assumed to be independent and identically distributed CSCG random variables i.e., $\mathrm{H}(f_l) \sim \mathcal{CN}(0, \sigma_h^2)$ (for Rayleigh fading) and $\mathrm{n}(f_l) \sim \mathcal{CN}(0, \sigma^2)$. 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 $\boldsymbol{\kappa} = [\kappa_1, \kappa_2 \cdots \kappa_L]$ 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 channel phases accounted in the proposed scheme provide more secure encryption compared to the gain, due to their sensitivity and unpre-

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

dictable nature to the locations of transceivers. Then, the transmitted signal in the physical layer response is represented as follows:

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

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

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

where $\tilde{\theta}_l = \theta_l - \hat{\theta}_l$ and $\mathrm{n}(f_l)$ 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 $\boldsymbol{\kappa}_{AB}$ 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 $\boldsymbol{\kappa}_E$. In [8], the test statistics of $\zeta = |\boldsymbol{\kappa}_{AB} \mathbf{Y}_R^T|$ is used for binary hypothesis testing. Here, $\mathbf{Y}_R = [Y_R(f_1), Y_R(f_2), \cdots, Y_R(f_L)]$ 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, of which details will be 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 binary decision for conventional PLA, whether the received signal is legitimate one 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 a high probability. On the other hand, in 'Gray', the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

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 that is hard to make a firm decision in 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 a 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 among '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

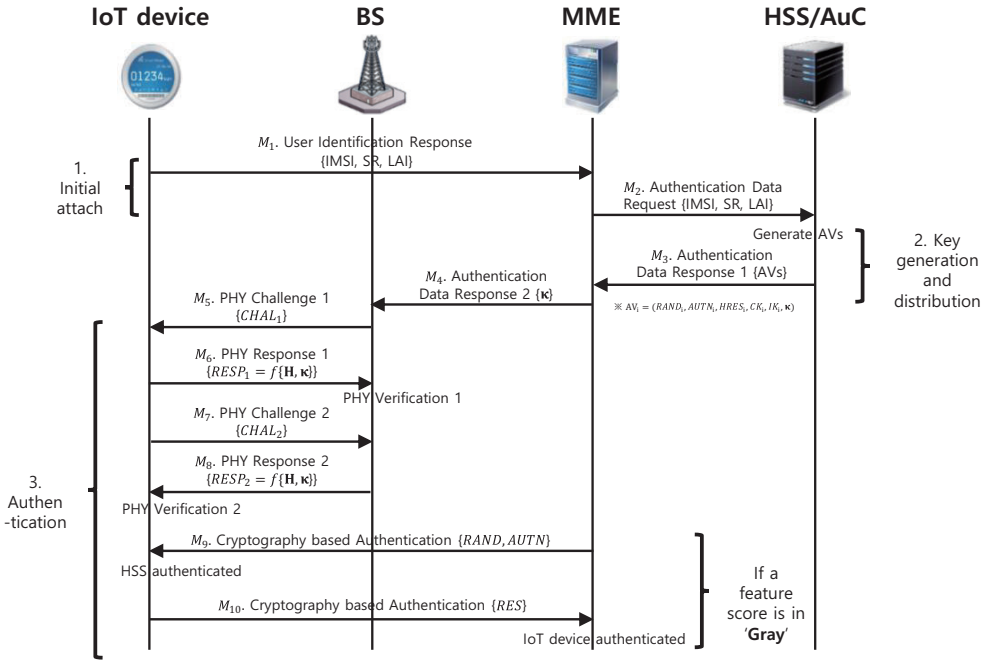

Figure 1. PL-AKA cross-layer authentication protocol [17]

Based on the integration strategy, detailed procedures of the proposed PL-AKA 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.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

- 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 one from 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 is how to integrate PLA with cryptography-based authentication. To this end, as shown in the Figure 1, the PHY-CRAM method is employed as a 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.

4. Performance Analysis

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

$$P_E = \rho P_M + (1-\rho)P_F \tag{5}$$

where P_M and P_F are the miss and false alarm probabilities at the BS, respectively, and ρ is a weighting factor ($0 \le \rho \le 1$). Note that $P_E = 0$ is assumed in the conventional cryptography-based authentication. PM is the probability that when the legitimate IoT device transmits, the BS decides that the signal is an intrusion signal and PF 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:

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

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

where $\nu_i = \mathbb{E}[\zeta|\mathcal{H}_i]$, $\sigma_i^2 = \mathrm{Var}[\zeta|\mathcal{H}_i]$ 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:

$$\alpha_1 = \underset{\alpha}{\mathrm{argmax}}\, F_{\zeta|\mathcal{H}_1}(\alpha) \le P_M^\circ \tag{8}$$

$$\alpha_0 = \underset{\alpha}{\mathrm{argmax}}(1 - F_{\zeta|\mathcal{H}_0}(\alpha)) \le P_F^\circ \tag{9}$$

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

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

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	$608 + L$

can induce a large signaling overhead. we compare the proposed protocol with the conventional EPS-AKA protocol in terms of 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:

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

Note that the lower target miss and false alarm probabilities is set, the larger the distance between α_1 and α_0 which determines the range of '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

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

In [19], the signaling overhead of EPS-AKA is given

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

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

$$\mathbb{E}[\Omega_{PL-AKA}] = N(\sum_{m=1}^{8} |M_m| + \tilde{\lambda} \sum_{n=9}^{10} |M_n|) + N(P-1)(|M_1| + \sum_{p=5}^{8} |M_p| + \tilde{\lambda} \sum_{q=9}^{10} |M_q|) \tag{13}$$

$$\mathbb{E}[\Omega_{PL-AKA_{MME}}] = N(\sum_{m=1}^{4} |M_m| + \tilde{\lambda} \sum_{n=9}^{10} |M_n|) + N(P-1)(|M_1| + \tilde{\lambda} \sum_{q=9}^{10} |M_q|) \tag{14}$$

where M_i is the i^{th} message in the proposed protocol. Based on the related parameters in TABLE I, $|M_1| = |M2| = 176$, $|M_3| = 608U + L$, $|M_4| = |M_5| = |M_6| = |M_7| = |M_8| = L$, $|M_9| = 288$, and $|M_{10}| = 64$. The signaling overhead of the PL-AKA depends on L and λ determined by P_M° and P_F°.

We present simulation results to see the authentication and signaling overhead performances of the proposed protocol. For simulations, we assume $\sigma_h^2 = 1$. SNR is defined 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 = 5dB. As shown in the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

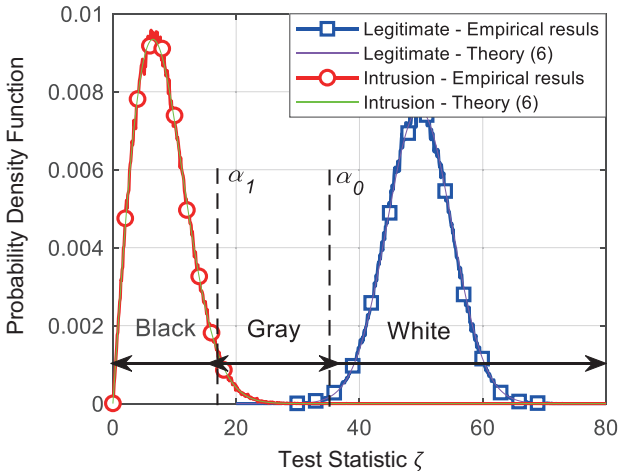

Figure 2. Comparison of the probability density functions and signaling overheads

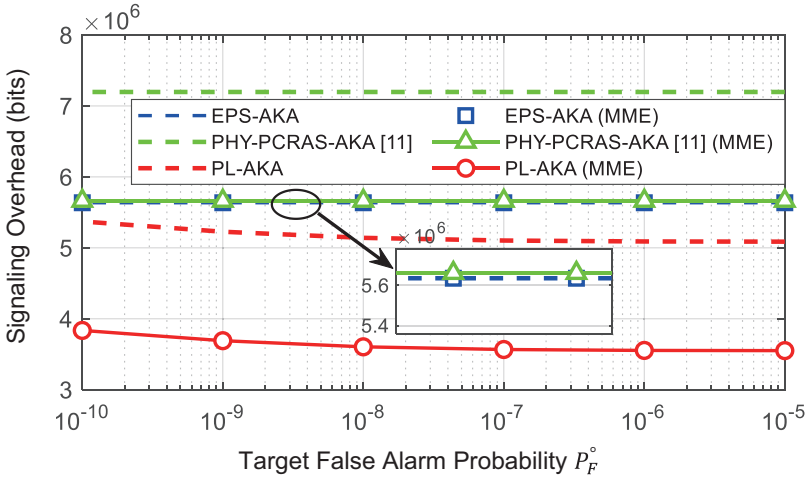

Figure 3. Comparison of the probability density functions and signaling overheads

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

Figure 2, the distribution of $\zeta|\mathcal{H}_1$ from the legitimate device is sufficiently distinguishable from that of $\zeta|\mathcal{H}_0$ from 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 the 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}) will be 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 simulation, signaling overhead is divided into two types: i) total signaling overhead, ii) signaling overhead at MME. As shown in the Figure 3, although $P_M^\circ = 10^{-10}$, the proposed PL-AKA has small total signaling overhead, compared to the conventional methods. In particular, the PHY-PCRAS-AKA [11] needs larger signaling overhead than EPS-AKA because it simply cascades both layer authentication methods for enhancement of security. Furthermore, while signaling overhead at MME is same as the total signaling overhead in the conventional EPS-AKA, in the proposed PL-AKA, signaling overhead at MME is significantly smaller than total signaling overhead because the BS performs a preemptive authentication instead of the MME in the proposed PL-AKA protocol.

4.2. Experiment Analysis

In this subsection, we implement an experiment to demonstrate practical performance of the proposed PL-AKA. To this end, the test statistics is measured in an actual LTE communication environment using USRP. Then, based on the acquired measurements, a probability of 'Gray' (i.e., λ) and signaling overhead are calculated. With considering the channel reciprocity from a previous work [20], we simply suppose that an BS transmits the challenge signal to a user equipment (UE) for PHY-CRAM.

4.2.1. Experiment Setup

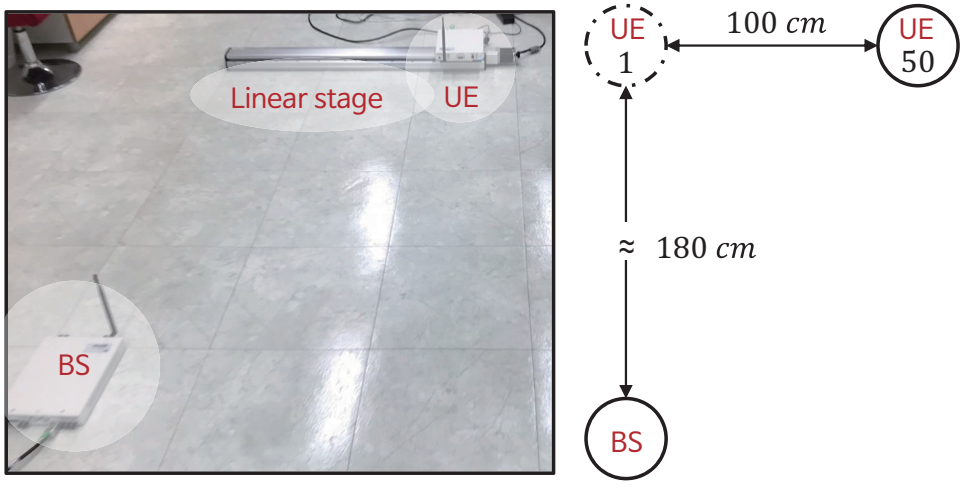

Figure 4. Experiment setup for measuring physical channels

Figure 4 illustrates experimental environment. The experiment is designed with 2 NI-USRP 2944R and LTE application framework running on Labview NXG 4.0 of National Instrument. The specifications of USRP 2944R is indicated in Table 2. The Host-PC is Dell Insprion 3650 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 a motorized linear stage with Autonics PHC-1HS-USB controller. UE moves 50 locations that apart from 2

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

cm 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 hours, and communication parameters are indicated in Table 3.

Table 2: USRP 2944R specifications

Transmitter	
Frequency range	10 MHz to 6 GHz
Frequency step	< 1kHz
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	< 1kHz
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

In practical communication, information of a channel phase loses the quality as a distinguished feature for PLA due to a carrier frequency offset (CFO) and sampling timing offset (STO). For this reason, sanitized channel phase ($\bar{\theta}$) [21] is exploited to obtain a fingerprint. Utilizing the sanitized phase, RMSD can also be a simple alternative test statistic instead of [8]. Let denote RMSD as η, which is defined with the following equation:

$$\eta_k^{(L_i,L_j)} = \text{RMSD}(\bar{\boldsymbol{\theta}}_{Ref}^{(L_i)}, \bar{\boldsymbol{\theta}}_k^{(L_j)}) = \sqrt{\frac{\sum_{r=1}^{n}\left(\bar{\theta}_{Ref,r}^{(L_i)} - \bar{\theta}_{k,r}^{(L_j)}\right)^2}{n}} \tag{15}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

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 1^{st} frame from a location i is selected to the reference frame $\tilde{\boldsymbol{\theta}}_{Ref}^{(L_i)}$.

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 Intercarrier Dependency

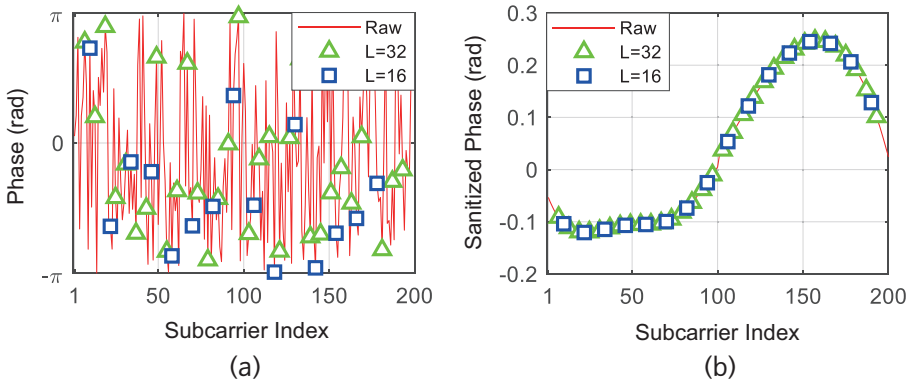

Figure 5. Raw and irregularly sampled channel phase profiles of (a) independently simulated and (b) USRP experimented correlated channels

Another constraint that arises in measuring test statistics is intercarrier dependency. Figure 5 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 whole CRS subcarrier to encapsulate secret key. This result implies that however a number of subcarriers are used, there is no significant reliability increase, but it improves a secrecy ability with the extension of the key length. From the point of view of reliability and computational efficiency, selective subcarrier benefits from signaling overhead but it has to sacrifices a secrecy ability.

4.6. Experimental Results

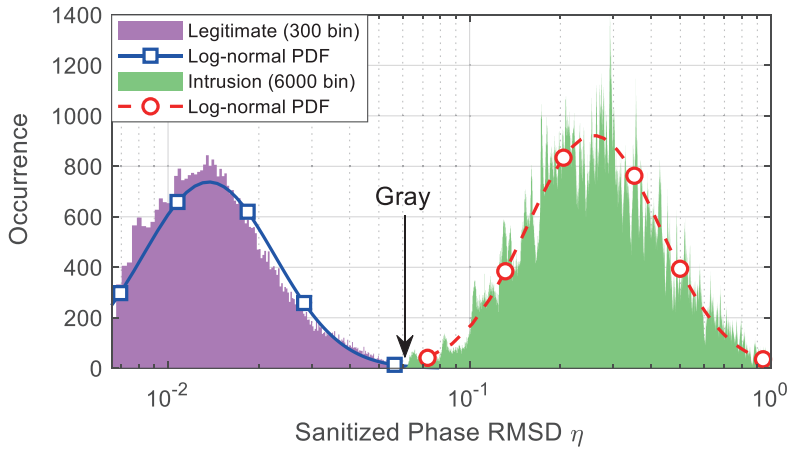

Figure 6. Histogram of sanitized phase RMSD η

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

Figure 6 is the histogram of RMSD results of the experiment. For ease of comprehension, we assume that the profiles can be fitted as log-normal distribution i.e., $\ln(X) \sim (\nu_i, \sigma_i^2)$ that PDF and CDF are defined by

$$f_{\eta|\mathcal{H}_i}(x) = \frac{1}{x\sigma_i\sqrt{2\pi}} e^{-\frac{(\ln x - \nu_i)^2}{2\sigma_i^2}}, \quad x > 0 \quad \text{and} \quad i = 0, 1 \tag{16}$$

$$F_{\eta|\mathcal{H}_i}(x) = \frac{1}{2} + \frac{1}{2}\text{erf}\left(\frac{\ln x - \nu_i}{\sqrt{2}\sigma_i}\right) \tag{17}$$

where $\nu_i = \mathbb{E}[\eta|\mathcal{H}_i]$, $\sigma_i^2 = \text{Var}[\eta|\mathcal{H}_i]$ and erf(x) is error function [22] respectively. From above equations, P_M°, P_F° and λ can be induced by applying the concept in equation (8), (9) and (10) conversely. Then, in case of RMSD, thresholds are determined as follows:

$$\alpha_1 = \underset{\alpha}{\text{argmax}}(1 - F_{\eta|\mathcal{H}_1}(\alpha)) \leq P_M^\circ \tag{18}$$

$$\alpha_0 = \underset{\alpha}{\text{argmax}}\, F_{\eta|\mathcal{H}_0}(\alpha) \leq P_F^\circ \tag{19}$$

As shown in Figure 7, 'Black', 'Gray' and 'White' are determined as follows:

$$\Theta = \begin{cases} \text{Black} & \text{if} \quad \eta > \alpha_1 \\ \text{Gray} & \text{if} \quad \alpha_0 \leq \eta \leq \alpha_1 \\ \text{White} & \text{if} \quad \eta < \alpha_0 \end{cases} \tag{20}$$

Figure 8 shows that the signaling overhead of conventional EPS-AKA and proposed PL-AKA in different numbers of subcarriers and target false alarm rates, where $P = 30$, $U = 20$, $N = 200$, $P_M^\circ = 10^{-6}$. In addition, we investigated not only the signaling overhead of total protocol, but also that of MME as described in (14). Although proposed scheme has the inefficient performance when $P_F^\circ = 10^{-10}$, $L = 64$ 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 target false alarm rate. Thus, the number of subcarrier and false alarm and miss detection probability should be coordinated moderately as its application.

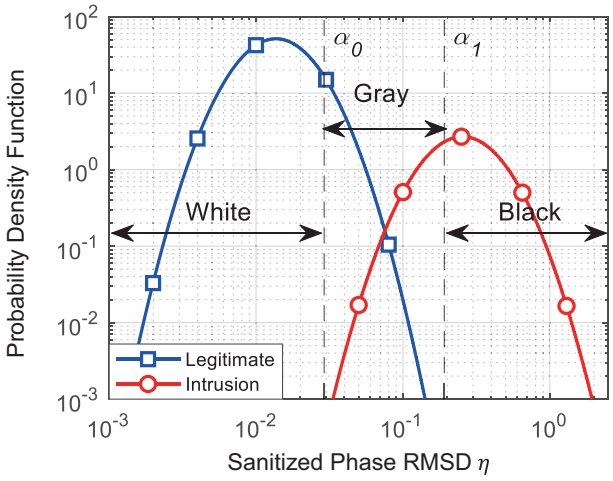

Figure 7. PDFs of RMSD for PL-AKA

5. Conclusion

In this paper, we presented lightweight PL-AKA protocol by applying PLA to conventional AKA protocol, preemptively. To this end, we considered the integration strategy

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2021 doi:10.20944/preprints202107.0013.v1

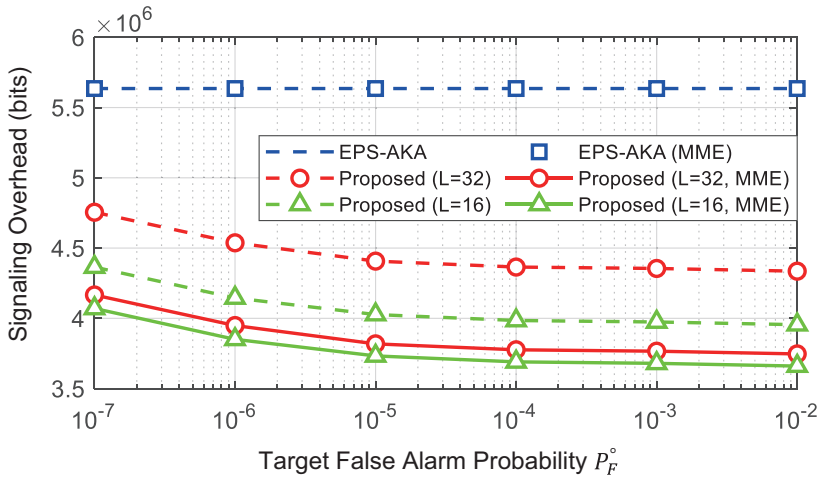

Figure 8. Signaling overheads of PL-AKA and EPS-AKA over various target false alarm probabilities

of the PLA and conventional cryptography-based authentication, classifying the PLA results to 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, USRP-based experimental analysis is conducted to demonstrate the proposed scheme in practical application for IoT. In this analysis, we installed BS and UE as LTE communication system, and observing the CSI according to physical location with linear stage. Here, phase sanitization is introduced to neutralize the effect of CFO and STO, and RMSD is defined to separate the legitimate and intrusion channel. In conclusion, the proposed scheme can achieve efficient signaling overhead than conventional schemes in both simulation and experimental results. There are some challenges discouraging the proposed scheme from practical implementation such as high 'Gray' probability and trade off between security and reliability. To solve this, machine learning-based PHY feature extraction or employment of multiple PHY attribute can be future works.

Author Contributions: S.H contributed towards 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 conceptualization, methodology, experimental analysis, validation, review and editing. and E.H proofread, conceptualization, methodology, formal analysis, review and editing as the corresponding author and provided guidance throughout the whole preparation of the manuscript.

Funding: This research was funded by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2017-0-00413, Streamlined Secure Communications by Physical Layer Identification in Cellular IoT).

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: Data available on request due to restrictions eg privacy or ethical The data presented in this study are available on request from the corresponding author. The data are not publicly available due to [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.

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. 2015 IEEE seventh international conference on intelligent computing and information systems (ICICIS). IEEE, 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 Transactions on Smart Grid* **2018**, *10*, 4349–4359.
4. Modiri, M.M.; Mohajeri, J.; Salmasizadeh, M. GSL-AKA: Group-based secure lightweight authentication and key agreement protocol for M2M communication. 2018 9th International Symposium on Telecommunications (IST). IEEE, 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 of Things Journal* **2015**, *3*, 408–417.
6. Liu, Y.; Chen, H.H.; Wang, L. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Communications Surveys & Tutorials* **2016**, *19*, 347–376.
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.
8. Wu, X.; Yang, Z. Physical-layer authentication for multi-carrier transmission. *IEEE Communications Letters* **2014**, *19*, 74–77.
9. Wu, X.; Yang, Z.; Ling, C.; Xia, X.G. Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission. *IEEE Transactions on Wireless Communications* **2016**, *15*, 6611–6625.
10. Shan, D.; Zeng, K.; Xiang, W.; Richardson, P.; Dong, Y. PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks. *IEEE Journal on selected areas in communications* **2013**, *31*, 1817–1827.
11. Wu, X.; Yang, Z.; Ling, C.; Xia, X.G. A physical-layer authentication assisted scheme for enhancing 3GPP authentication. *arXiv preprint arXiv:1502.07565* **2015**.
12. Wen, H.; Wang, Y.; Zhu, X.; Li, J.; Zhou, L. Physical layer assist authentication technique for smart meter system. *Iet Communications* **2013**, *7*, 189–197.
13. Moreira, C.M.; Kaddoum, G.; Bou-Harb, E. Cross-layer authentication protocol design for ultra-dense 5G HetNets. 2018 IEEE International Conference on Communications (ICC). IEEE, 2018, pp. 1–7.
14. Abdelaziz, A.; Koksal, C.E.; Burton, R.; Barickman, F.; Martin, J.; Weston, J.; Woodruff, K. Beyond PKI: Enhanced authentication in vehicular networks via MIMO. 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). IEEE, 2018, pp. 1–5.
15. Marcus, M.J. 5G and" IMT for 2020 and beyond"[Spectrum Policy and Regulatory Issues]. *IEEE Wireless Communications* **2015**, *22*, 2–3.
16. Cao, J.; Ma, M.; Li, H. LPPA: Lightweight privacy-preservation access authentication scheme for massive devices in fifth Generation (5G) cellular networks. *International Journal of Communication Systems* **2019**, *32*, e3860.
17. Lee, Y.; Hwang, E.; Choi, J. Physical layer aided authentication and key agreement for the Internet of Things. 2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS). IEEE, 2020, pp. 1–7.
18. Nutall, A.H. Some integrals involving the QM function. *IEEE Trans. Information Theory* **1975**, *21*, 95–96.

 doi:10.20944/preprints202107.0013.v1

19. Lai, C.; Li, H.; Li, X.; Cao, J. A novel group access authentication and key agreement protocol for machine-type communication. *Transactions on emerging telecommunications technologies* **2015**, *26*, 414–431.
20. Han, S.; Lee, Y.; Hwang, E. Experimental analysis on secret key generation scheme based on wireless channel state information using USRP. *Proc. Korean Inst. Comms Info. Sci. (KICS)* **2019**, pp. 302–303.
21. Qian, K.; Wu, C.; Yang, Z.; Liu, Y.; Zhou, Z. PADS: Passive detection of moving targets with dynamic speed using PHY layer information. 2014 20th IEEE international conference on parallel and distributed systems (ICPADS). IEEE, 2014, pp. 1–8.
22. Chang, S.H.; Cosman, P.C.; Milstein, L.B. Chernoff-type bounds for the Gaussian error function. *IEEE Transactions on Communications* **2011**, *59*, 2939–2944.