A Cross-layer Collaborative Handover Authentication Approach for 5G Heterogeneous Network

Ting Ma1,* and Feng Hu2

1School of Electrical and Information Engineering, Southwest Petroleum University, Sichuan, China
2School of Electrical and Information Engineering, Suzhou Vocational University, Jiangsu, China

*E-mail: mating@swpu.edu.cn

Abstract. The next fifth generation mobile network (5G) is going to have a massive impact on almost new frontier technological applications in everything from smartphones to future vehicles, with highly heterogeneous, broadband access everywhere, faster speeds, lower latency and higher throughput. As moving to 5G, security architecture must also evolve, especially to seek for more efficient and secure handover authentication solutions. In this work, we design our security mechanism based on physical layer and upper layer cryptographic techniques, combining the advantages of these techniques to achieve a faster and more reliable authentication objective for 5G HetNets. In the cross-layer authentication solution, we firstly execute the handover authentication in physical-layer. Kolmogorov-Smirnov (K-S) hypothesis is adopted by exploiting the physical layer attributes of wireless channels. If it pass the initial authentication, then we implement the EAP/AKA authentication to achieve a more reliable security objective. Finally, the numerical simulation results and discussions are presented to show the feasibility of the proposed approach.

1. Introduction

The mobile data traffic is dramatically increased as anywhere and anytime wireless connectivity has become a reality in the recent few years. In the near future, some service scenarios such as autonomous driving vehicles, smart building, Internet of Things (IoT), and many other diverse user applications will result in an explosive increase of data traffic. The exponential growth of mobile traffic poses a stringent and urgent problem in the definition and development on the future 5G mobile networks [1]. 5G aims to achieve various attractive features, including the capability to support device to device (D2D) communication, to provide higher network capacity than 4G cellular network, and to serve mobile users with higher density [2]. In order to provide ubiquitous high-rate and seamless communication service, concepts of femtocells, microcells and relays are proposed, including massive multiple-input-multiple-output (MIMO) [3]. As a result, new technologies and application architectures in 5G will pose new challenges in security issue and use privacy protection. Since 5G network is heterogeneous and users join and leave more frequently in small cell, the handover authentication should be improved. Handover authentication and privacy protection approaches with low latency and robustness need to be developed for 5G HetNets.

Ensuring security of 5G HetNets has become increasing significant. To provision confidentiality, the typical solution is through upper-layer cryptographic protocols. The cyclic redundancy check
(CRC) technique is widely used. Dubrova et al. propose to use CRC to detect messages with double-bot errors [4]. The CRC codes is based on hash function. To implement the CRC codes, a linear feedback shift register (LFSR) is employed. However, the LFSR requires additional programmable and re-programmable connections. In [5], a pseudonymous authentication scheme is presented to provide secure and data confidentiality video reporting service in 5G vehicular networks. The proposed cryptographic solutions include a public key encryption, an attribute-based encryption and a pseudonymous authentication. However, it is complex to perform the cryptography for networks with limited computational and bandwidth resources.

Recently, research interest is growing in physical layer authentication by exploiting unique and inherent physical layer information. In contrast of conventional cryptographic approaches, physical layer authentication makes use of channel state information of communication channels to discover malicious attacks at less computational cost and is considered to deliver fast and efficient performance [6], [7]. Channel-based fingerprinting is the major research objective for many existing physical layer authentication schemes. Channel state information (CSI), the carrier frequency offset (CFO), the channel impulse response (CIR) and the receiving signal strength (RSS) can be employed to distinguish signals from an authorized transmitter and unauthorized transmitters [8], [9], [10], [11]. In these schemes, a suitable threshold is selected to achieve a successful detection in a sophisticated hypothesis test, like Neyman-Pearson test [12] and the binary test with Kalman Filter [13]. Particularly, by using RSSI signal, Liang et al. propose a logistic regression-based physical layer authentication to provide online authentication [14], which is claimed more efficient and secure than the conventional cryptographic scheme. However, this work is relying on the known channel model.

However, it is not robust and reliable to only rely on one physical layer attribute, since the chosen attribute may not have enough dynamic range. In order to achieve a more reliable security objective, we need to combine both the physical layer authentication and upper layers security together. With these considerations, in this paper, we will introduce a cross-layer collaborative authentication method to greatly reduce the time delay and computational complexity in comparison to traditional cryptographic methods. Additionally, our proposed technique adopts the more universal nonparametric Kolmogorov-Smirnov (K-S) test in the physical layer authentications. This is because the distribution forms of the physical layer attributes (PLAs’) diverse from scenario to scenario. The rest of this paper is organized as follows. Section 2 briefly introduces 5G network model. In Section 3 we provide a detailed description of the proposed cross-layer collaborative authentication scheme. Simulation results are reported in section 4 and our conclusions are drawn in Section 5.

2. 5G network model

The software-defined networking (SDN) enabled 5G network model is illustrated in Figure 1. The SDN controller embedded with the authentication management module (AMM) has global control over the whole 5G HetNets. The evolved network nodes (eNBs) and access points (APs) serve as the access nodes and they operate under the rules defined by the network controller. More specifically, all involved switches, the access points (APX) and the base stations (eNBX) forward their data through SDN protocols like Openflow and Simple Network Management Protocol (SNMP) [14]. More precisely, the AMM is implemented in the network controller to achieve seamless handover authentication. When a user firstly launch to the network, it will undergo a full authentication, such as the Extensible Authentication Protocol (EAP). Then AMM collects and analyses the physical layer attributes (PLAs) of the user by using specific protocols like traffic flow template (TFT). Besides, the SDN controller inspects and predicts the user location and prepares the relevant eNBX and APX for fast user connection. Thus, a SDN-enabled network is capable of facilitating 5G HetNets communication more efficiently.
3. The cross-layer collaborative authentication scheme

3.1 Physical-layer authentication

As a mean of non-cryptographic method, physical layer authentication exploits channel specific features for identities verifications and attack detections. Specifically, user specific physical layer characteristics are regarded as a unique digest of the specific user. The legitimate receiver can quickly distinguish between authorized and rogue transmitter by performing physical layer authentication. Physical layer authentication simplifies traditional authentication procedures in a lower computational cost manner. Physical layer authentication is especially suitable for 5G heterogeneous network with minimal overhead and low latency.

A mathematical model is established to facilitate the physical layer authentication analysis. Since the quality of the user equipment (UE)-AP mutual information keeps changing all the time, the PLAs of a specific UE served by the AP can be modelled as statistical variables. Here use the vectorised form of $x = [x_1, x_2, \ldots, x_j, \ldots, x_d]^T$ for these statistical variables, where $d$ denotes the number of available PLAs of the UE. Assume that the AMM maintains $N$ samples of the statistical vectors. The sampled PLA matrix can be defined as

$$S_r = \begin{bmatrix} x_1, x_2, \ldots, x_j, \ldots, x_N \end{bmatrix}$$  \hspace{1cm} (1)$$

When a handover is initialized, the AMM will collect another $N$ samples of PLAs for authentication. The PLA matrix for text can then be written as

$$S_t = \begin{bmatrix} x'_1, x'_2, \ldots, x'_j, \ldots, x'_N \end{bmatrix}$$  \hspace{1cm} (2)$$

Hence, the spoofing detection process can be simplified as: with the knowledge of $S_r$ and $S_t$, the AMM should detect whether they belong to the same UE. The mathematical model diagram for physical layer authentication process is illustrated in detail in Figure 2.

According to the aforementioned discussion, the PLAs’ distribution is unknown to the AMM. Then, we assume $x \sim f_r(\theta_r)$ and $x' \sim f'_r(\theta'_r)$ in the presence of $S_r$ and $S_t$, where $f_r$ and $f'_r$ are distribution function arrays which represent the PDFs of the UE’s PLAs and the distribution characteristic parameters are denoted as vectors $\theta_r$ and $\theta'_r$ respectively. Hence, the authentication model can be expressed as the following hypothesis test:
To be more specific, the hypothesis test can be abstracted as: when the distribution characteristic parameters are almost the same, we have hypothesis \( H_0 \); otherwise, hypothesis \( H_1 \) is acceptable if the distribution characteristic parameters are against a predefined threshold. Besides, from aforementioned definitions, we can see that the hypothesis test avoid quantitative estimation of \( \theta_r \) and \( \theta_t \). Consequently, the non-parametric K-S theory test is more suitable for networks with less parameter constraints. In this paper, we adopt K-S theory as the hypothesis test [15].

Subsequently, the empirical cumulative distribution functions (CDFs) of the \( i^{th} \) physical layer attribute from \( S_r \) and \( S_t \) can be described by

\[
F_{i,r}(x) = \frac{1}{N} \sum_{j=1}^{N} I_{[-\infty,x]}(x_{i,j})
\]

\[
F_{i,t}(x) = \frac{1}{N} \sum_{j=1}^{N} I_{[-\infty,x]}'(x_{i,j}')
\]

where \( I_{[-\infty,x]}(x_{i,j}) \) is the indicator function. We can consider that the indicator function is equal to 1 if \( x_{i,j} \leq x \) and is equal to 0 otherwise. The K-S statistic for the \( i^{th} \) attribute can be written as

\[
D = \sup_{x} \left| F_{i,r}(x) - F_{i,t}(x) \right|
\]

The decision threshold and the decision rule can be described by

\[
D \leq c(\alpha) \sqrt{\frac{2}{N}}
\]

where \( \alpha \) is the confidence level and \( c(\alpha) \) can be calculated according to

\[
c(\alpha) = \sqrt{-\frac{1}{2} \ln \frac{\alpha}{2}}
\]
During the authentication, each available PLAs need to be checked by the K-S test illustrated above. In order to achieve a more robust authentication performance, a voting rule is implemented in the final decision: the majority is adopted. The proposed K-S test based physical layer authentication procedure can be summarized and shown in Figure 3.

**Figure 3. Physical layer authentication procedure.**

### 3.2 Cross-layer authentication

Generally, cryptography techniques can achieve highly security objectives such as data confidentiality, non-reputation and data integrity. However, it comes at a cost of computation complexity and overhead for verification and authentication. It is especially not suitable for networks with dynamics features and low latency requirements. Physical layer authentication has the advantage of providing security without higher-layer encryption. It reduces complexity and overhead since it exploits inherent characteristics that are already existing at the terminals. Additionally, it is very difficult for an attacker to replicate the diverse features to launch a spoofing attack. However, because physical layer authentication relies heavily on channel characteristics, it might not suitable for implementation in weak channel scenario. By jointly considering these circumstances, we propose a cross-layer collaborative authentication mechanism, combining the advantages of upper layer and physical layer authentication to reduce latency and enhance the robustness of the authentication process as a double security insurance.

UE and the AP first to perform the K-S test physical layer authentication procedure based on the channel information attributes. If the UE has not passed the physical layer authentication, a faster security objective is achieved at the signal level with no additional upper layer authentication, significantly reducing authentication delay and computational overhead. Otherwise, if the UE has successfully passed the physical layer authentication, then UE and the AP continue to implement the EAP/AKA authentication to achieve a more reliable security objective. The proposed cross-layer authentication process framework is illustrated in Figure 4.

### 4. Performance evaluation

#### 4.1 Resource cost
4.2 Numerical results and discussions

Simulations are performed with MATLAB to evaluate the proposed authentication procedure. Based on the discussion above, the proposed K-S test is applicable to PLAs authentication when the distribution of PLAs is unknown. In the Simulations, we evaluate the performance of K-S test under different physical layer attributes scenarios. For the first scenario, we consider RSS difference authentication as discussed in [9]. In the simulation, we set $\sigma = 1.3$ for when legitimate user exists, and $\sigma = 9$ for scenario with illegal users, where the parameter $\sigma$ reflects the RSS difference distribution. The detection performance of authentication is evaluated by Receiver Operating Characteristic (ROC) curve, which reflects the relationship between successful authentication rate and false authentication rate. With different training size $N$, Figure 5 shows the ROC curves of the proposed authentication solution. We can see that a larger $N$ contributes to a lower identification error. For instance, the training size $N$ should be at least 20 to meet an 80% detection rate and the false alarm rate can be kept below 1%.

The second simulation is performed to evaluate our proposed scheme in the authentication scenario based on CFO, where the assumptions in [17] are used. A uniform distribution in the range of [-200,200] kHz is assumed for the CFO of the illegal users while the CFO of the legitimate users is set as 20 kHz. As the signal to noise ratio (SNR) can affect the CFO detection, the training sequence size $N$ can be increased to compensate introduced performance degradation. Figure 6 illustrates the improvement on the false alarm rate ($P_f$) with increasing $N$. The false alarm rate is defined as the probability of rejecting a legal user. In this simulation, we set $\alpha = 0.001$ for loose decision threshold. As shown in figure 6, higher SNR results in better authentication performance. It can be observed that the proposed authentication scheme achieves a high authentication rate with a small number of training data. In addition, the ROC curves for CFO verification under our proposed scheme are shown in figure 7. We set SNR to 5 dB in this simulation. It can be seen that a larger training size results in a more accurate detection performance. For instance, with 10 samples of training data, a detection rate above 80% is achieved with a $P_f$ as low as 1.3%.
Figure 5. Simulated ROC curves for RSSI authentication.

Figure 6. Simulated false alarm rate versus SNR under different training data size.

Figure 7. Simulated ROC curves for CFO authentication.
The presented two numerical simulation results demonstrate that the proposed authentication can achieve a low false acceptance rate and high successful authentication rate under various physical layer attributes.

4.3 Network performance
As the mobility and number of user equipment will increase dramatically in the 5G scenario, future 5G network is supposed to support massive handover operations more frequently. Assume a number of $N_{auth}$ handover authentications should be processed by the AMM during a specific time slot, within which a $p$ percentage handover requests are from legal users, the total processing time of the proposed cross-layer authentication scheme can be written as

$$t_{proc} = N_{auth} \{t_{ks} \ast tpr \ast p + (t_{ks} + t_{eap})\} \{p(1-tpr) + (1-p)\}$$

(9)

where $tpr$ is the true positive rate of the physical layer K-S test; $t_{ks}$ and $t_{eap}$ are the processing time for physical layer K-S authentication and upper layer EAP/AKA authentication respectively. In order to enhance the network security, the false positive rate of the K-S test should be maintained to be zero in our proposed authentication scheme. For such purpose, the K-S test parameter in equation (8) is carefully chosen. The handover processing time of the proposed cross-layer authentication scheme is simulated and the result is shown in Figure 8. The simulation parameters are based on [9]. The processing time is normalized to the traditional EAP/AKA based authentication scheme. It is observed that with the percentage of legal user increase, the handover processing time of the proposed authentication scheme decrease, resulting in a more efficient network performance. It is also shown that a larger $N$ (number of frames used for physical layer K-S test) corresponds to a better network performance enhancement. As a matter of fact, the key parameter that determines the network performance is the true positive rate $tpr$ of the K-S test.

![Figure 8. Simulated handover processing time of the proposed cross-layer authentication scheme by using RSSI in the physical layer K-S test.](image)

5. Conclusion
In this article, an upper layer assisted physical layer authentication scheme is presented for SDN enabled 5G HetNets. Firstly, in the physical layer authentication, the nonparametric K-S test based authentication algorithm is developed. When served as an auxiliary authentication method, the adopted K-S test based scheme can generate reliable security performance. Furthermore, the EAP/AKA authentication is implemented to achieve a more reliable security objective. The performance of the proposed schemes has been demonstrated through numerical simulations. When compared with the
traditional cryptographic methods, the proposed authentication scheme performs with better efficiency in terms of computational resource requirement under 5G HetNets application.

Acknowledgments
This work was supported by the Young Scholars Development Fund of SWPU (No.201699010009).

References
[1] L. Qiang et al 2016 “A user centered multi-objective handoff scheme for hybrid 5G environments” IEEE Trans. on Emerging Topics in Computing, p.1-11
[2] C. I et al 2015 “The 5g huddle” IEEE Vehicular Technology Mag., p.28-31
[3] A. Gupta et al 2015 “A survey of 5g network: architecture and emerging technologies” IEEE Access, p.1206-32
[4] E. Dubrova et al 2015 “CRC-based message authentication for 5G mobile technology” Proc. IEEE Trustcom/BigDataSE/ISPA, p.1186-91
[5] M. H. Eiza et al 2016 “Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks” IEEE Trans. Veh. Technol. VOL.65 NO. 10, p.7868-81
[6] L. Xiao et al 2008 “Using the physical layer for wireless authentication in time-variant channels,” IEEE Trans. on Wireless Commun., VOL. 7 NO. 7, p. 2571-2579
[7] X.F. Wu et al 2015 “Physical-Layer Authentication for Multi-Carrier Transmission” IEEE Communication Letters, VOL. 19 NO. 1, p. 74-77
[8] X. Duan et al 2016 “Fast authentication in 5g hetnet through sdn enabled weighted secure-context-information transfer” Proc. IEEE International Conf. on Commun., p. 1-6
[9] K. Zeng et al 2010 “Non-cryptographic authentication and identification in wireless networks” Wireless Commun., VOL.17 NO. 5, p. 56-62
[10] F. J. Liu et al 2013 “A two dimensional quantization algorithm for cir-based physical layer authentication” Proc. IEEE International Conference on Communications, p. 4724-28
[11] A. Saud et al 2018 “Physical-layer entity authentication scheme for mobile MIMO systems” IEEE Trans. on Commun., VOL. 12 NO.6, p. 712-718
[12] Q. Wang 2017 “A novel physical layer assisted authentication scheme for mobile wireless sensor networks” Sensors (Basel), VOL.17 NO. 2
[13] X. Duan et al 2015 “Authentication handover and privacy protection in 5g hetnets using software-defined networking” IEEE Communications Magazine, VOL.53 NO.4, p. 28-35
[14] L. Xiao et al 2018 “Phy-layer authentication with multiple landmarks with reduced overhead” IEEE Trans. on Wireless Commu.VOL.17 NO. 3, p.1676-87
[15] B.W. Woodruff et al 1983 “A Modified Kolmogorov-Smirnov Test for Weibull Distributions with Unknown Location and Scale Parameters” IEEE Trans. On Reliability VOL.R-32 NO.2, p. 209-213.
[16] H. Peng et al 2013 “An enhanced cross-layer authentication mechanism for wireless communications based on per and rssi” Proc. 13th Canadian Workshop on Information Theory, p. 44-48
[17] W. Hou et al 2012 “Physical layer authentication in ofdm systems based on hypothesis testing of cfo estimates” Proc. IEEE International Conf. on Commun., p. 3559-63.