Physical-Layer Authentication for Wireless Security Enhancement: Current Challenges and Future Developments

Xianbin Wang *Senior Member, IEEE* , Peng Hao, *Student Member, IEEE* and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—While the open nature of radio propagation enables convenient "anywhere" wireless access, it becomes the root of security vulnerabilities of wireless communications. In light of this, physical-layer authentication, which is based on exploitation of dynamics of physical layer attributes, is emerging as an effective approach in enhancing wireless security. In this paper, we first review the existing physical-layer authentication techniques and identify their current limitations, ranging from the low authentication reliability to the difficulties of integrating these techniques with the existing wireless infrastructure and applying them in complex future networks. We then present three promising research areas in addressing these challenges. Specifically, we propose to use multi-attributes multi-observation (MAMO) technique for enhancing the authentication reliability. In order to apply point-to-point physical layer authentication techniques into existing wireless networks, we propose a cross-layer authentication approach relying on a composite security key (CSK) that can seamlessly integrate physical-layer and upper-layer authentication schemes. We also discuss the possible ways of invoking physical layer authentication for reducing both the complexity and latency of the security processes in complex heterogeneous networks with the aid of the proposed physical security context sharing (PSCS).**

***Index Terms*—Physical-layer authentication, cross-layer authentication, wireless security, key generation, 5G, authentication handover.**

I. Introduction

Authentication of a wireless device is conventionally handled above the physical layer using key-based cryptography. Although the effectiveness of such techniques has been proven, the security key distribution and management over dynamic wireless networks face a range of emerging problems. The timely sharing of security keys in highly complex networks supporting a large number of mobile and heterogeneous devices is becoming a new challenge. On one hand, the high computational cost of key generation/detection may result in excessive latencies in large-scale networks, which may become intolerable for delay-sensitive communications. On the other hand, the promise that the digital key cannot be computationally broken still remains mathematically unproven [1]. With the rapid growth of processing power, the time spent on cracking a digital security key could be remarkably shortened. Most importantly, attackers using unauthorized security keys cannot be easily detected when the physical layer attributes are disregarded, because user identifications and access rights are only validated through digital keys.

In contrast to the existing upper-layer security schemes, wireless transmitters can also be validated at the physical-layer by verifying the dynamic characteristics of the associated physical communication links and devices [2]–[6], i.e. through physical-layer authentication. The reciprocal channel properties and some of the analog front-end (AFE) imperfections of wireless transceivers constitute primarily two categories of physical-layer attributes for device authentication [2]. Compared to digital key based authentication, the specific physical-layer attributes are directly related to the communicating devices and the corresponding environment, which are extremely difficult to impersonate. Furthermore, both the channel and device imperfection estimation and compensation techniques constitute inherent functions of communications receivers exploited for improving the reception performance. As a benefit of this, physical-layer authentication can be accomplished without incurring additional security overhead.

In this paper, we first identify the technical challenges of physical-layer authentication in terms of their reliability and integration with the existing network infrastructure and protocols. Three promising directions of overcoming these challenges are discussed. Specifically, we propose to enhance the reliability of physical-layer authentication with the aid of a novel multi-attributes and multi-observation (MAMO) technique. Furthermore, we explore the inherent link attributes for physical-layer key generation in enabling the concept of the composite security key (CSK). In doing so, the physical-layer authentication can be efficiently integrated with existing cryptography-based infrastructures and protocols. Additionally, the authentication procedure of the future 5th generation (5G) heterogeneous networks may be simplified and enhanced by the proposed predicted physical security context sharing (PSCS).

II. Challenges for Physical-Layer Authentication

Disregard the extensive research attentions it has drawn, physical layer authentication is still far from its practical deployment due to several challenges. In this section, three challenges of physical-layer authentication are discussed in detail.

A. Low Reliability of Physical-Layer Authentication

In general, physical-layer authentication techniques can be classified as channel-based and AFE imperfection based ap-

X. Wang and P. Hao are with the Department of Electrical and Computer Engineering, Western University, London, Ontario, Canada (e-mail: xianbin.wang, phao5@uwo.ca).

L. Hanzo is with the School of Electronics and Computer Science, University of Southampton, United Kingdom (email: lh@ecs.soton.ac.uk).

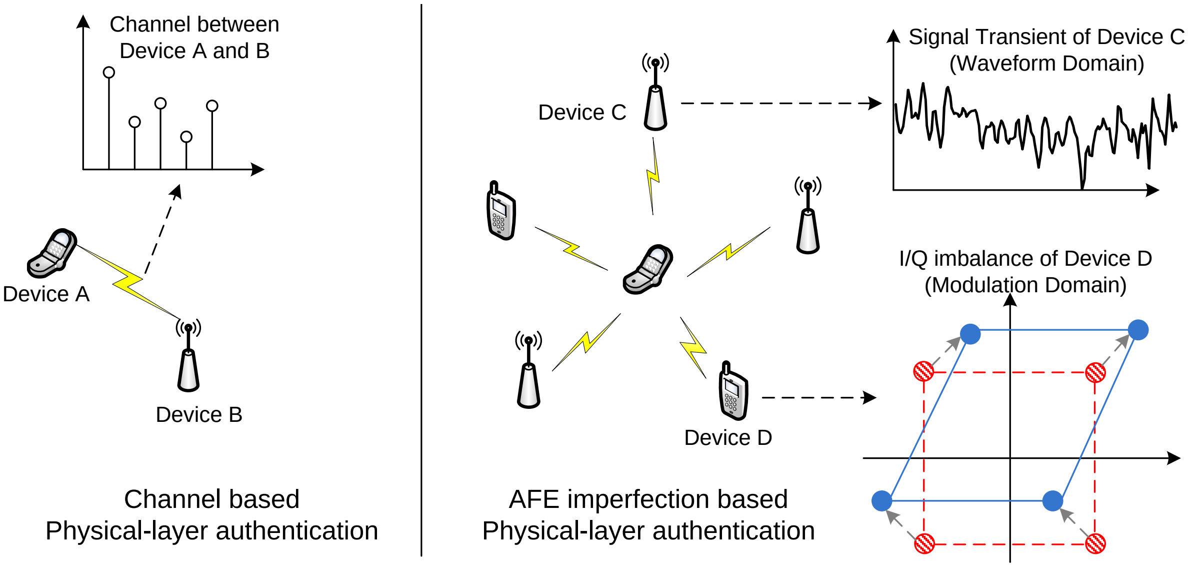

Fig. 1. Comparison of existing channel based and AFE imperfection based physical-layer authentication techniques.

proaches, as shown in Fig.1. The channel-based physical-layer authentication exploits the environment dependent radiometric features of a specific transceiver pair, such as channel state information (CSI) [3] or the received signal strength indicator (RSSI) [7]. These channel characteristics can be used for differentiating signals arriving from an authorized transmitter and that from spoofing transmitters. However, extensive channel monitoring and frequent adaptation of the authentication rules are required when the channel is non-stationary. This may become a challenge in highly dynamic environments (e.g., vehicle-to-vehicle communications) and in sleep-mode aided networks (e.g., IEEE 802.15.4 networks).

On the other hand, the attributes of the AFE may also be explored for authentication due to its relatively stable nature. These AFE imperfections are inevitable variations introduced to different devices during the fabrication of analog components. Several device-specific characteristics, including the in-phase/quadrature imbalance (IQI) [4], the digital-to-analog converter and the power amplifier characteristics [5], as well as the carrier frequency offset (CFO) [6] have been explored for authentication. In practice, the difference of the selected hardware attributes between different devices is usually small, and its observation is further corrupted by both the noise and the interference, which reduces the accuracy of estimating these attributes for authentication purposes.

B. Integration with the Existing Network Infrastructure and Authentication Protocols

Given the significant advantages of physical-layer authentication, it is straightforward to consider the integrated exploitation of physical-layer authentication as a complement to the upper-layer authentication schemes.

One of the most challenging tasks in cross-layer authentication is the integration of the physical-layer authentication with the existing infrastructure and protocols. In [2], an overview of cross-layer authentication by using lower/physical layer characteristics is provided. Some of the existing cross-layer schemes are implemented through quantization of physical-layer characteristics for upper-layer verification [8]. Although the authentication is realized at an upper layer, the principles of this kind of methods and of classic cryptography are rather different. Hence using it directly in a cryptosystem will impose additional cost and it is also likely to produce challenges.

Another related challenge is how to extend the device-to-device physical layer authentication to the more general scenarios of end-to-end authentication. In [9], a physical-layer key generation scheme exploiting the channel-reciprocity of the directly connected transmitter and receiver is discussed. However, in large-scale wireless networks, authentication and key exchange usually take place between devices which are not directly linked. By contrast, most of the current physical-layer authentication procedures are limited to device-to-device authentication, since they rely on the characteristics gleaned by analyzing the direct communication links between the transmitter and receiver. As a result, it is critical to develop authentication process, which is not restricted to the physical-layer of two directly communicating devices.

C. Authentication in Complex Heterogeneous Networks

It is anticipated that the operational wireless infrastructure will evolved into the 5G in supporting the dramatically increased tele-traffic. Given the significantly increased network complexity, mobile users will have to frequently switch between different base stations or access points, which results in frequent authentication handover. This situation becomes even more challenging in heterogenous networks (HetNet). The authentication handover is traditionally based on a cryptographic key and on multiple handshakes, as proposed by 3GPP committee in [10]. To seamlessly handover the entire context, the handover has to involve multiple entities including the users, APs, BSs and servers. Sophisticated backhaul processing and multiple handshakes have to be involved for information or pairwise key exchanges between these entities. In practice, all of these contribute to the unwanted latency. This procedure could take up to hundreds of milliseconds, which is far beyond the latency tolerance of 5G services [11].

III. Future Development of Physical Layer Security

In this section, we present three possible solutions in addressing the challenges identified.

A. Reliability Enhancement by Multi-Attribute Multi-Observation Authentication Techniques

As discussed earlier, the performance of physical layer authentication is often degraded by the instability of the rapidly time-varying channel. Additionally, the performance AFE imperfection based authentication techniques is limited by the low reliability of AFE imperfection estimation.

We propose to enhance the reliability of physical-layer authentication using MAMO techniques by exploitation of as many of the physical-layer attributes as possible for improving the authentication reliability. Indeed, various channel based and AFE imperfection based physical-layer characteristics may be readily combined for the environment-based characteristics, the CSI as well as some attributes like the RSSI, the round-trip time (RRT). As for hardware imperfection based characteristics, I/Q amplitude mismatch and phase shift error, the CFO and the clock skew etc. may be exploited.

The reliability of each physical layer attribute has to be taken into consideration for multi-attribute based authentication. The choice of using selected attributes for authentication depends upon the specific application scenarios. For instance, the time-invariant AFE imperfections constitute beneficial choices in mobile communications; the channel-based characteristics are expected to work well in stationary indoor scenarios. To elaborate further, we may consider the combination of multiple channel-based and AFE imperfection based characteristics for improved authentication performance since it is extremely unlikely for an attacker to occasionally experience the same communication channel and own nearly identical AFE imperfections as the legitimate transmitter. For example as studied in [15], optimal weights can be set for each of the selected attributes according to their reliability; the authenticity decision can be made either separately or totally based on all the selected characteristics.

The proposed multi-observation technique constitutes another approach of enhancing the characteristic estimation accuracy. Receiver diversity is an effective means of combating wireless fading, which improves the channel capacity by increasing the signal-to-noise-ratio (SNR). Given the fact that the estimated characteristics predetermine the attainable authentication reliability, it is plausible that the proposed multi-observation technique improves the authentication reliability. In a cooperative communication system, the source usually relies on multiple relays and optimal relay selection, which facilitates collaborative authentication strategy. For instance, many relays may receive an authentication request from the same source due to the broadcast nature of the wireless medium. Thus, the relays may rely on cooperative observations for jointly authenticating the transmitter for achieving improved authentication reliability.

B. Seamless Integration with Existing Networks and Protocol using Composite Security Key

To achieve effective integration of physical layer authentication and existing network and protocols, two key issues should be considered. Firstly, the proper choice of the physical-layer characteristics that can be extracted for upper-layer security mechanisms. Due to end-to-end nature of upper-layer authentication, duration of such procedure may be significant. Thus, only stable characteristics which are stationary during the authentication process can be exploited. Secondly, how to process the selected characteristics is another critical concern. The utilization of physical-layer characteristics in widely used symmetric/asymmetric key generation algorithms is an important area for further investigation.

In this subsection, we aim at addressing the problems in seamlessly integrating the physical-layer and existing upper-layer authentication schemes. We assume that the Device B needs to authenticate the claimed identity of Device A, while Device A and B are in end-to-end communication scenario as shown in Fig.2. Device C, which can be a collaborative access point in practice, is a trusted third party of Device B that shares the direct link with A.

The physical-layer of our design, which is at the bottom of the protocol stack, plays the critical role of providing characteristics including IQI, CFO, and even antenna-specific characteristics to the upper-layers.

The proposed authentication framework is summarized as follows. As a benefit of direct communication with Device A, Device C becomes capable of evaluating the physical-layer characteristics of A by analyzing its received signals. Therefore, the Device A-specific characteristics can be quantized and hashed at Device C for generating specific digital numbers (i.e. PHY-key), which are shared with both Device A and B for further authentication-related processing. Specifically, these PHY characteristic-related numbers of Device A can then be used for generating an asymmetric key for authentication purposes in this paper. The PHY-key related to Device A can be utilized in the existing key generation algorithm at Device A to generate an enhanced asymmetric key pair. The input from the physical layer, actually the PHY-key via Device C, can be used as partial input to the private key selection in the existing key generator, thus leading to physical-layer-dependent composite public and private key pair. On the other hand, the PHY-key can also be directly combined with the original public key from the existing key generator. This will lead to a composite public key, which is capable of preventing unauthorized decryption and cryptanalysis. In this case, additional decryption steps will be required in removing the effect of PHY-key. After generating the composite security keys, the public-key can be shared with B with the aid of the existing protocol, while the associated private key is only stored in Device A without being shared with any other devices. Basically, Device A uses its private key to encrypt a

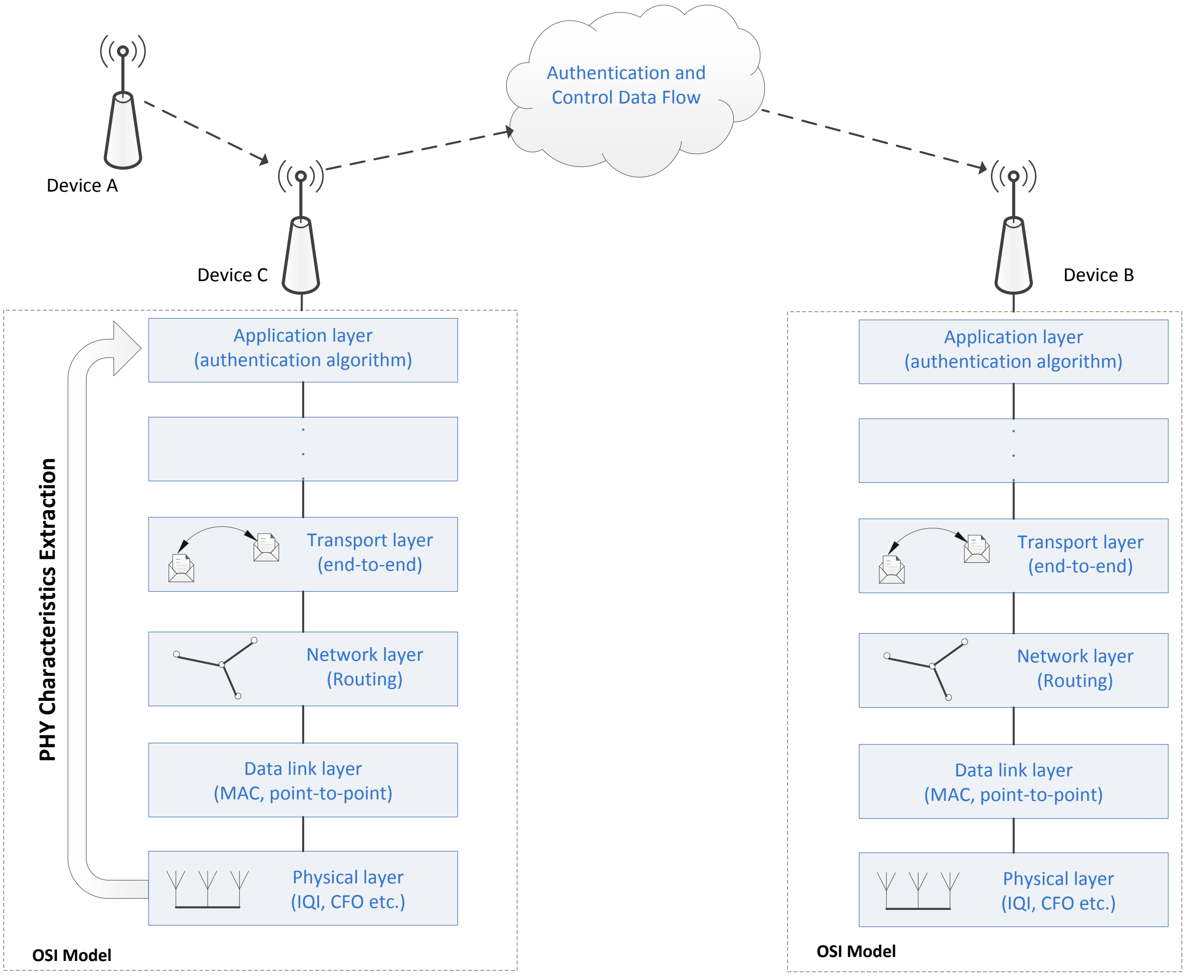
Authentication and Control Data Flow
Device A
Device C
Device B
PHY Characteristics Extraction
Application layer (authentication algorithm)
Transport layer (end-to-end)
Network layer (Routing)
Data link layer (MAC, point-to-point)
Physical layer (IQI, CFO etc.)
OSI Model
Application layer (authentication algorithm)
Transport layer (end-to-end)
Network layer (Routing)
Data link layer (MAC, point-to-point)
Physical layer (IQI, CFO etc.)
OSI Model

Fig. 2. Cross-layer design for end-to-end authentication.

plaintext and to generate the corresponding ciphertext. Device B attempts to decrypt the ciphertext using the public key, while the authenticity of A is verified only if B is capable of decrypting the readable digest, since only A owns the private key. It is worth noting that PHY-key generation exploiting the hardware-imperfection related attributes is typically more stable than those gleaned from the wireless channels as argued in [9]. The input from the physical layer expressed in term of the total number of bits used in the CSK can be adjusted according to the robustness of the physical layer attributes. In addition, mutual authentication may also be realized through the utilization of the shared secret key between A and B with the aid of collaborative devices, e.g. Device C for Device A.

There are two main benefits of using the proposed PHY-key and composite security key. On the one hand, the proposed method could be more efficient. Existing approaches directly using these physical-layer characteristics as an authentication tag will pose additional payload at each layer's data encapsulation and cost additional bandwidth and power in delivering them to Device B. Comparatively, using these characteristics as securing key can eliminate this overhead. On the other hand, the robustness of authentication process is enhanced. Similar to the two-factor authentication strategy in which the physical possession factor and virtual password factor are checked together as a double insurance, the PHY-key and CSK are also secured by the intrinsically unforgeable feature of physical-layer characteristics and the computational intractability of asymmetric encryptions.

C. Authentication Handover Simplification using Physical Security Context Sharing

In this subsection, we focus on simplifying the authentication procedure in the complex 5G HetNet. The prediction and sharing of physical-layer attributes as security context are the two key aspects of our solution. As illustrated in Fig.3, we assume a user is moving between cells.

Security Context Prediction. The variation trend of attributes such as direction of arrival (DOA), RSS, RTT and CSI can be used for physical security context, which can be further predicted based on their previous observations and plays important role in simplifying authentication handover. For example, with the predicted DOA, the authentication-oriented beams of BS or AP can accurately point to the antenna array of the intended user, which actively prevents the imper-

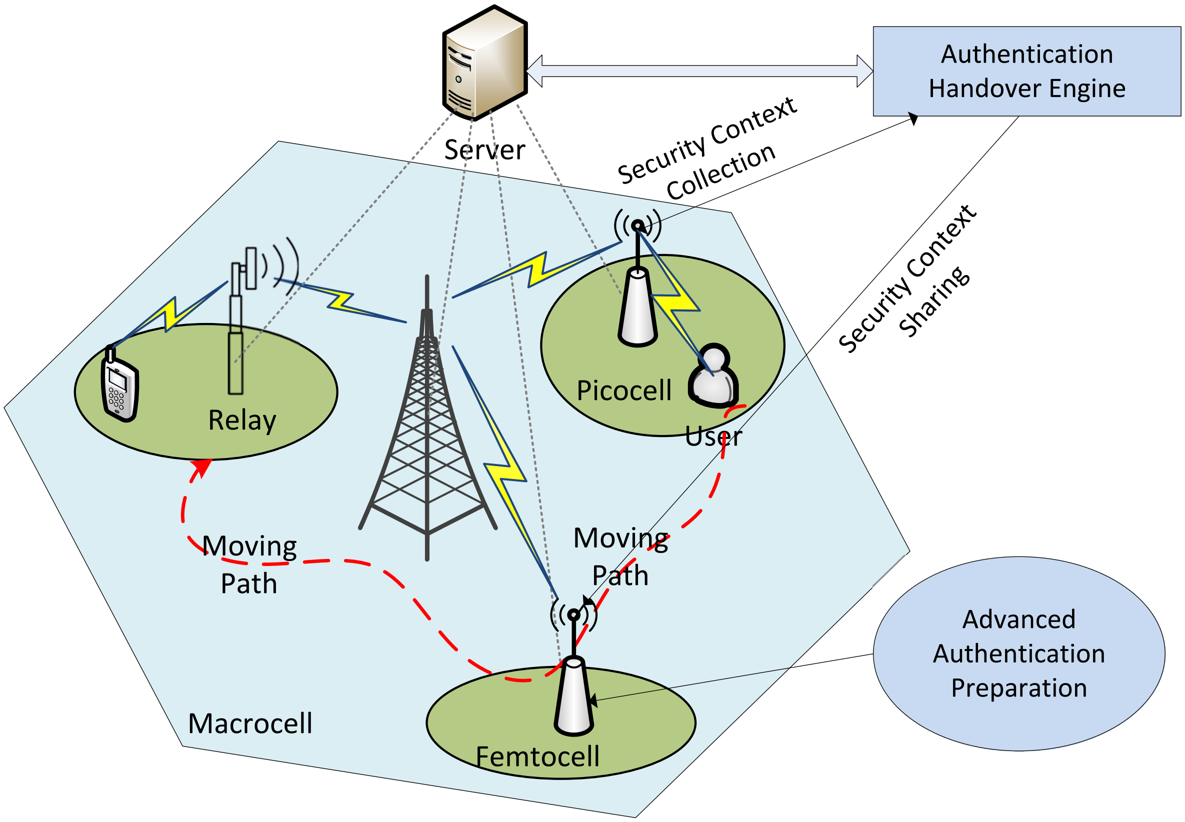
Server
Authentication Handover Engine
Security Context Collection
Security Context Sharing
Relay
Picocell
User
Moving Path
Moving Path
Advanced Authentication Preparation
Macrocell
Femtocell

Fig. 3. Simplification of authentication handover with physical security context prediction and sharing.

sonation attacker from the highly directional communication link between the user and BS/AP. Besides, these attributes can also be used to monitor and track the real-time moving direction and position of the user. The next cell that the user will enter can be consequently predicted. The authentication server thereby is able to prepare the authentication related information (e.g., the PHY-key information) and send them to the serving AP of the next cell in advance. Once the user enters the new cell, the authentication and association request can be responded immediately by the serving AP. It is noteworthy that the emerging SDN can be utilized to efficiently manage the network-wide authentication information as proposed in [13].

Security Context Sharing. With increased network complexity and operating frequency, more physical characteristics and security context can be observed and shared for authentication purpose. The authentication handover may not happen in a completely new context, implying many of the already known information of the stable and predictable characteristics can be reused. For example, the PHY-key has high potential to be used as a network-wide unique and unforgeable key because we involved the physical-layer factors into the key generation. In this case, some repetitive steps such as the frequently repeated pairwise key generation in the solely cryptographic authentication schemes can be reduced.

IV. Case Study and Performance Evaluation

A. Case Study I: Relay Authentication using Multi-Characteristics and Diversity Technique

In the first case study, we consider the authentication of amplify-and-forward (AF) relay as a special case. The AF relays, also known as analog repeater, only work at physical layer and thereby cannot adopt most of the upper-layer authentication schemes. We here apply and evaluate the solely physical-layer level authentication reliability enhancement using the proposed MAMO technique.

The combination of channel based RSSI and AFE imperfection based IQI may be readily considered as a benefit of their availability in most of wireless receivers. The RSSI is a representative of the level of the received radio signals and can be directly accessed at physical-layer [7], [14]. Regarding the IQI, we use the same model as in [4], where the AF relay involves one receiving IQI component and one transmission IQI component. For simplicity, we denote the four characteristics of IQI as $[\alpha_r, \theta_r, \alpha_t, \theta_t]$, where α and θ represent the amplitude and phase shift imbalances, while the subscripts r and t denote reception and transmission. Our objective is to authenticate AF relay nodes by the joint verification of their RSSI and IQI.

The proposed authentication procedure is evaluated using MATLAB simulations. We consider four legitimate AF relays and an illegitimate AF relay with α and θ randomly chosen from $-0.05 \sim 0.05$ and $-5^o \sim 5^o$, respectively. The RSSI readings of each AF relay are obtained from the experiments using Atheros WiFi devices [14]. We randomly choose one AF relay in each round of simulations and estimate the corresponding IQI and RSSI of this relay. The generalized likelihood ratio test and hypothesis testing is applied first to determine the relay's authenticity based on the IQI and RSSI separately. Eventually, we combine the two attributes for the final authentication decision. Specifically, we claim having a legitimate relay only when both the IQI and RSSI based tests claim the same legitimate relay nodes. Additionally, 3 antennas are assumed at receiver in demonstrating the benefits of multi-observation based authentication enhancement by using maximal ratio combining (MRC) of multiple received signals. The probability of correct authentication vs. false alarm rate is shown in Fig.4, where the probability of correct authentication is defined as the percentage of successful authentication trials in the total number of authentication tests. It becomes explicit that the probability of correct authentication is significantly improved by using multiple characteristics (i.e., RSSI and IQI) and MRC-based hypothesis testing. To be specific, the proposed MAMO technique provides on average a 9.28% and 50.48% higher correct authentication probability than conventional authentication techniques, when only IQI is used in isolation with and without MRC, respectively. This is because the combined characteristics are more reliable and distinguishable than a single characteristic. Additionally, the accuracy of estimating multi-characteristic is further enhanced by combining multiple observations through MRC.

B. Case Study II: Cross-layer Authentication using PHY-Key

In this case study, our proposed cross-layer authentication is evaluated in terms of correct authentication probability and delay reduction.

We first apply the proposed PHY-key into the existing one-way hash digital signature authentication scheme. The block diagram is shown in Fig.5. For simplicity, we also use IQI to generate the PHY-key in this case study. Without loss of generality, we consider general transmitter rather than AF relay so that the IQI is modeled as $[\alpha_t, \theta_t]$. As shown in this figure, the message-digest 5 (MD5) is used as the hash function to process the quantized IQI and to generate the 128-bit hash value; the RSA algorithm is used for processing the outputs of compositing procedure in order to generate the public and private keys as we presented in Section III. The MRC relying on multiple antennas is also considered at the receiver to increase the IQI estimates-to-noise ratio.

Additionally, we also simulated the proposed authentication simplification in a handover scenario with using the PHY-key. For description simplicity, we assume user U moves to a new cell covered by B from the cell covered by A, while A and B are severed by server S. The identity of U has been authenticated by A, i.e., A has the knowledge of U's identity either as a legitimate user or an impersonation attacker. We also assume an authorized devices list $AUTH$ and an attackers list $ATTK$ kept at A, B and S as $(AUTH, ATTK)_A$, $(AUTH, ATTK)_B$ and $(AUTH, ATTK)_S$, respectively. The lists contain the information of identity, PHY-key and some predicted direction and position of different users. Our handover procedure with the prediction and reuse of these lists is presented in Algorithm1.

Algorithm 1 Authentication handover using PHY-key

```
1) Start of the authentication handover procedure.
2) A shares the $(AUTH, ATTK)_A$ about U to B directly or via S. B updates $(AUTH, ATTK)_B$.
3) U sends B the association request with claimed identity and signature using the above-mentioned one-way hash method.
4) B first checks $AUTH_B$. If U is in $AUTH_B$, B uses the corresponding public-key to decrypt the received signature. If it can decrypt correctly, go to step 7); if it is incorrect, go to step 5). If U is not in $AUTH_B$, go to step 5).
5) B generates PHY-key of U and checks $(ATTK)_B$. If U is in $(ATTK)_B$, go to step 7). If U is not in $(AUTH, ATTK)_B$, B sends S the PHY-key of U, then go to step 6).
6) If S decides to grant U the access, go to 7); otherwise, go to 8).
7) B grants U the access in the response, and go to 9).
8) B rejects U in the response.
9) B shares the updated $(AUTH, ATTK)_B$ about U to the next possible cell based the prediction.
10) End of authentication handover.
```

The simulation results on authentication probability vs SNR and handover delay are shown in Fig.6. We can see that the probability of correct authentication of our cross-layer authentication increases with the SNR and it can be further improved using MRC. It can also be observed that the correct authentication probability is higher than 97%, even when the SNR is as low as 10 dB, which is a representative of relatively poor wireless communication scenario. For characterizing handover latency, we simulate our handover simplification method and compare it to the traditional handover scheme. The traditional handover scheme of [13] relying on [10] proposed by 3GPP is used in this investigation. In the traditional handover, a highly authentication-induced processing delay is imposed by the handover-related request, response and handshake procedures. In this figure, it can be seen that the delay of both methods is increasing when network utilization rate (NUR) becomes higher, where NUR is defined as the ratio of actual network traffic to the maximum traffic that the network can handle. We can observe that the handover delay for both methods stays low if NUR is below 60%. When the network-load becomes high, our method shows its superiority in reducing the delay. Compared to the traditional method, the delay is reduced as we pre-share the $(AUTH, ATTK)$ of user by relying on the prediction at step 2) and reuse the shared information at step 4).

V. Conclusions

This article focused on the current challenges and future development of physical-layer authentication techniques. We identified three main challenges of physical-layer authentication development in terms of the relatively low authentication reliability, seamless integration with existing upper-layer authentication protocols and the increased authentication

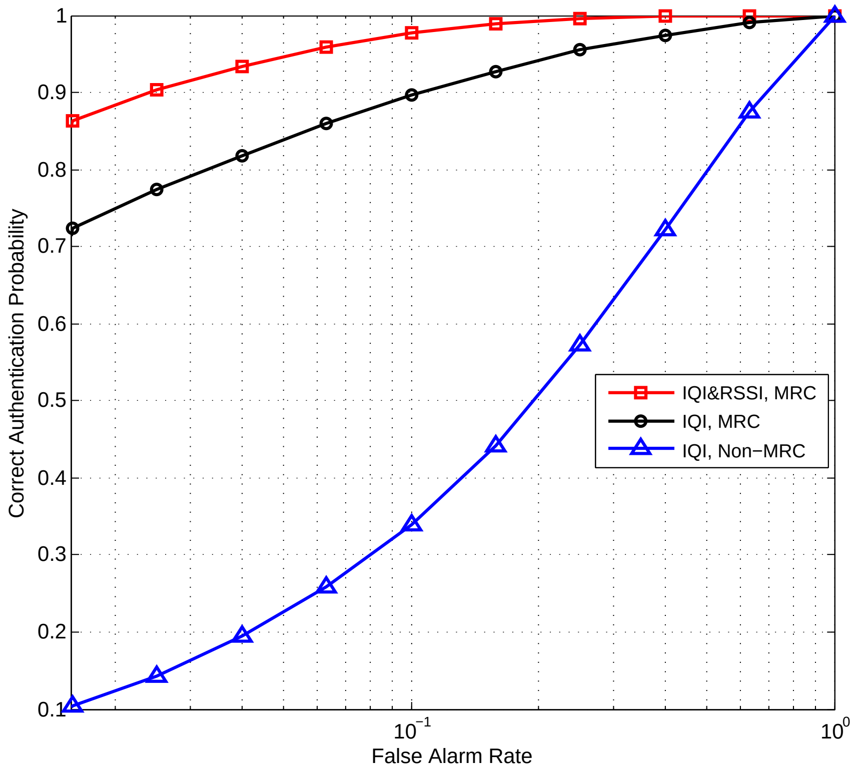

Fig. 4. Authentication performance using multiple physical layer attributes.

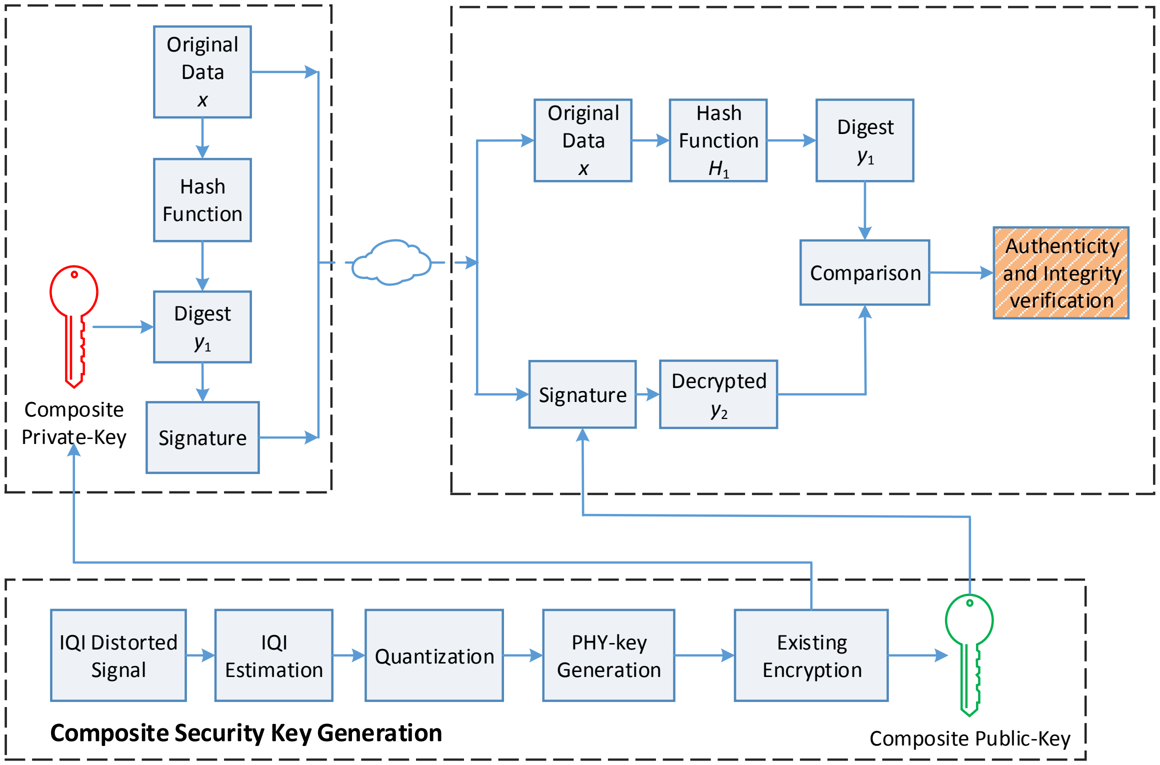

Fig. 5. One-way hash digital signature using PHY-key generation.

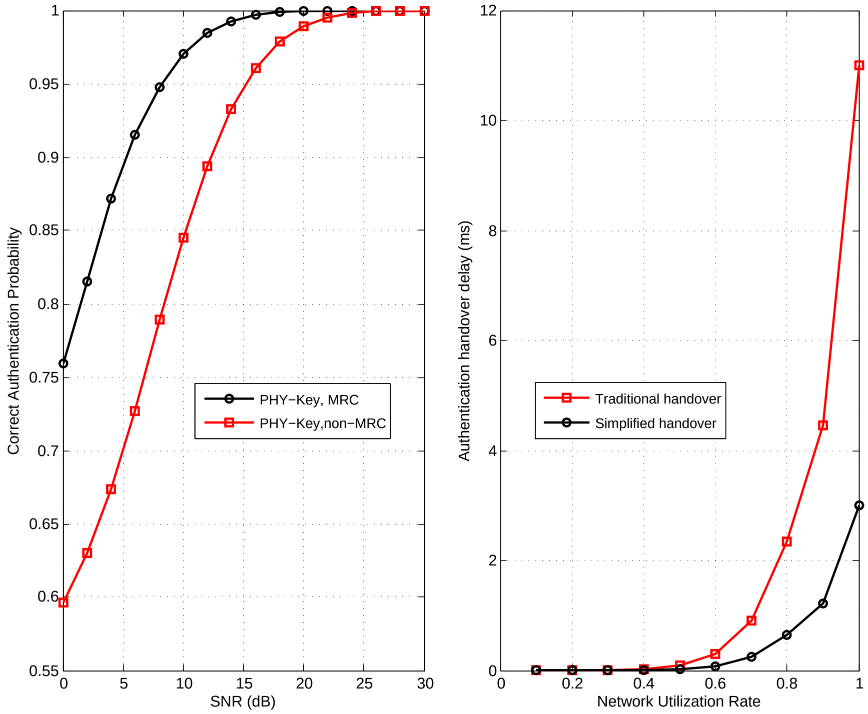

Fig. 6. Probability of correct authentication using PHY-key and handover delay.

complexity problem in 5G. We then proposed three solutions to deal with these problems. Specifically, we proposed the MAMO techniques to enhance the reliability of physical layer authentication. Also, we propose the cross-layer aided architecture as well as PHY-key and Composite Security Key generation to achieve seamless integration of physical-layer authentication and cryptography schemes. It is noteworthy that the brute-force search attack, which is the weakness of traditional cryptography, can be effectively alleviated by using the PHY-key. In addition, the upcoming 5G will bring fundamental impacts to current physical-layer authentication due to increased network complexity. New security approaches including the proposed physical layer security context predication and sharing has been studied in simplifying authentication handover in 5G.

References

[1] A. Mukherjee, S.A.A. Fakoorian, H. Jing, and A.L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, 2014, pp.1550-1573.

[2] K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," *IEEE Wireless Commun.*, vol. 17, no. 5, 2010, pp. 56-62.

[3] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, "Using the Physical Layer for Wireless Authentication in Time-variant Channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, 2008, pp.2571-2579.

[4] P. Hao, X. Wang, and A. Behnad, "Relay Authentication by Exploiting I/Q Imbalance in Amplify-and-Forward system," *in Proc. IEEE Conf. on Global Commun. (GLOBECOM)*, Dec. 2014, pp.613 - 618.

[5] A.C. Polak, S. Dolatshahi, and D.L. Goeckel, "Identifying Wireless Users via Transmitter Imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, 2011, pp.1469 - 1479.

[6] W. Hou, X. Wang, J.Y. Chouinard, and A. Refaey, "Physical Layer Authentication for Mobile Systems with Time-varying Carrier Frequency Offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, 2014, pp.1658 - 1667.

[7] Y. Chen, Y. Jie, W. Trappe, and R.P. Martin, "Detecting and Localizing Identity-based Attacks in Wireless and Sensor Networks", *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, 2010, pp.2418-2434.

[8] B. Vladimir, B. Suman, G. Marco and O. Sangho, "Wireless Device Identification with Radiometric Signatures," *in Proc. ACM Int. Conf. on Mobile Computing and Networking (MobiCom)*, 2008, pp.116-127.

[9] K. Zeng, "Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, Jun. 2015, pp.33-39.

[10] 3GPP TS 33.401 V11.5.0. 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 11), 2012.

[11] D. He, C. Chen, S. Chan, and J. Bu, "Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions", *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, 2012, pp.48-53.

[12] J.G. Andrews, S. Buzzi, C. Wan, S.V. Hanly, A. Lozano, A.C.K. Soong, and J.C. Zhang, "What will 5G be?", *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, 2014, pp.1065 - 1082.

[13] X. Duan and X. Wang, "Authentication Handover and Privacy Protection in 5G HetNet using Software-Defined Networking," *IEEE Commun. Mag.*, vol. 53, no. 4, Apr. 2015, pp.28 - 35.

[14] P. Hao, X. Wang, and A. Refaey, "An Enhanced Cross-layer Authentication Mechanism for Wireless Communications based on PER and RSSI," *in Proc. IEEE Canadian Workshop on Info. Theory (CWIT)*, Jun. 2013, pp.44 - 48.

[15] P. Hao and X. Wang, "Performance Enhanced Wireless Device Authentication using Multiple Weighted Device-specific Characteristics," *in Proc. IEEE China Summit & Intl. Conf. on Signal and Inf. Process. (ChinaSIP)*, Jul. 2015, pp.438 - 442.