IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON MOBILE MULTIMEDIA: METHODOLOGY AND APPLICATIONS

Received November 7, 2019, accepted November 24, 2019, date of publication November 28, 2019,
date of current version December 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2956480

Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks

XIAOYING QIU[1], (Member, IEEE), ZHIGUO DU[2], (Student Member, IEEE), AND XUAN SUN[1], (Member, IEEE)

[1]School of Information Management, Beijing Information Science and Technology University, Beijing 100192, China
[2]School of Information Technology and Cyber Security, People's Public Security University of China, Beijing 10038, China

Corresponding author: Xiaoying Qiu (qxy@bupt.edu.cn)

This work was supported by the National Key Research and Development Program of China under Grant 2018YFC0824405-03.

ABSTRACT Security provisioning has become a key issue in wireless multimedia networks due to their vital roles in supporting various services. Conventional security solutions have deficiencies in computing efficiency and addressing emerging security challenges. In addition, traditional upper-layer authentication ignores the protection of the physical layer, leading to severe privacy data leakage. In this paper, we envision a new deep learning (DL)-enabled security authentication scheme to overcome these issues, while implementing Blind Feature Learning (BFL) and Lightweight Physical Layer Authentication (LPLA). Specifically, an intelligent authentication method is developed by exploring neural networks at the data collection unit to learn the characteristics of data. Then we propose a holistic authentication scheme based on machine learning to identify malicious multimedia devices. Experimental analysis verifies that the proposed scheme can guarantee the privacy of wireless multimedia sensors and achieve lightweight authentication. Performance results indicate that artificial intelligence-enabled authentication scheme improves the overall security of multimedia networks.

INDEX TERMS Multimedia network, machine learning, security, neural network.

I. INTRODUCTION

The advent of technologies in 5G and Internet of Things (IoT) heralds the arrival of the next wave of ubiquitous connected society [1]–[5]. In particular, multimedia networks and their ongoing convergence with artificial intelligence technologies are widely expected to bring exciting services and applications for monitoring, entertaining, training, and operating in the areas of smart home, smart city, healthcare, transportation, and so on [6], [7]. Multimedia applications will greatly expand the way humans perceive the world and be widely applied to people's daily lives.

However, the complexity of multimedia systems as well as dramatically increasing use of multimedia sensors within smart processes bring many security and privacy challenges. For example, when multimedia nodes collect various data through different sensors, the malicious sensors could deceive users by exploiting interactivity and providing false message in the systems [8], [9]. Potential security risks and attacks could lead to catastrophic consequences and cause avalanche-like damages in wireless multimedia networks [10]. Moreover, the widely used resource-constrained multimedia devices are vulnerable to attacks, causing widespread distributed threats to multimedia networks through data injection, spoofing, and eavesdropping. Therefore, it is necessary to design an effective protection mechanism for wireless multimedia networks to ensure the security of communication transmissions. Usually, authentication and access control techniques are considered as key security mechanisms and critical designs for multimedia paradigm, since adversary attackers need the access requirements of multimedia resources [11]. These techniques secure legitimate communications by confirming the identities of all users and their access to the authorized network. However, the particularity of a large number of multimedia devices poses new design challenges for security configurations. Explicitly, those multimedia devices claiming low-delay transmissions could not support the authentication methods

The associate editor coordinating the review of this manuscript and approving it for publication was Dapeng Wu.

that require high computational overhead, and tremendous sensors contained in a wireless multimedia system require lightweight computing costs to ensure their communication performance. Hence, in order to defend against the threat of attacks in wireless multimedia networks, this paper focuses on the challenges faced by traditional authentication schemes, and further proposes new security enhancement methods.

A. CHALLENGES FOR CONVENTIONAL SECURITY APPROACHES

Conventional key-based cryptography techniques require significant resource and high computing capability, which is inefficient for wireless multimedia communication networks [12]. More importantly, digital key may be compromised in security management procedures, such as key distribution. The challenges faced by conventional authentication schemes are summarized as follows.

1) UNBALANCED GROWTH IN LOW COMPUTATIONAL COSTS AND HIGH SECURITY

Traditional security solutions may suffer from adversary attacks in complex multimedia communication scenarios due to the increasing number of multimedia sensors and the wide range of applications. Security methods implemented on higher layers are difficult to overcome the conflict between costs and security, resulting in failure to protect legitimate communications. The malicious devices may steal sensitive data through forged public keys and seriously damage the authentication mechanism. Therefore, new concepts based on artificial intelligence-assisted lightweight authentication are extremely beneficial for overall security in a wireless multimedia environment.

2) COMPLEX AUTHENTICATION PROCESS INDUCED LATENCY IN REAL-TIME MULTIMEDIA NETWORKS

Traditional authentication techniques require more effort to extract complex features to increase the level of security, resulting in higher communication and computation overheads and, what's worse, longer communication latency. This is unbearable for wireless multimedia networks with significantly increasing number of smart multimedia sensors and resource-constrained wearable nodes. In addition, the conventional statistical schemes for authentication also require sufficient time to manually select the fixed statistical characteristics, thus leading to a non-adaptive authentication process. As a result, a new adaptive authentication scheme is necessary for security application scenarios.

3) INACCURATE PREDICTIONS DURING THE SECURITY AUTHENTICATION PROCEDURE

Conventional authentication techniques are also difficult to establish an accurate detection model in an unpredictable communication environment. Statistical hypothesis testing may use limited statistical properties to predict outcomes. These have brought huge loopholes to the learning model and also pose a potential security threat to continuous authentication. In order to improve the security of the authentication process, it is necessary to design an intelligent authentication approach that does not require explicit programming.

In short, security authentication is critical for wireless multimedia networks, especially in the information age of the Internet of Everything.

B. OUR CONTRIBUTIONS

To address these challenges, we use artificial intelligence algorithms to perform Lightweight Physical Layer Authentication (LPLA) for wireless multimedia networks. Aiming at the security authentication issue of multimedia devices, a physical attribute selection method based on blind feature learning is proposed. In summary, our contributions are as follows.

- We discuss the challenges and potential solutions for sybil detection mechanisms in wireless multimedia communications. In particular, we build machine learning-based detection mechanisms by exploiting physical layer attributes. As recent studies demonstrate, physical layer channels are incredibly portable, simple, and efficient, without causing additional computational overheads and communication latency, thus suitable for lightweight security authentication of wireless multimedia networks.
- We design an artificial intelligence-based model for extracting the authentication attributes without requiring the channel variation pattern, and cast the authenticator from the statistical feature space to the blind learning feature space. The learning-enabled authentication process is then viewed as a classification system that is easier to train based on physical layer controllable parameters and test results. As a result of this characteristic transformation, the complexity of our learning-based authentication model can be significantly reduced, despite the consideration of high-level of physical layer properties.
- Our numerical performance and simulations results verify that the proposed blind feature learning selection of channel attributes can significantly improve the authentication performance without excessively reducing the convergence and training performance. We also demonstrate the advantages of artificial intelligence assisted physical layer authentication scheme over other non-feature selection techniques.

C. ORGANIZATION

The rest of this paper is structured as follows. Section II summarizes the related work. Section III gives a description of the system model in this paper. Section IV describes an overall authentication scheme based on artificial intelligence techniques. Section V introduces numerical analysis and security performance. Section VI describes the future research prospects. Finally, this paper is concluded in Section VII.

II. RELATED WORK

Security authentication and artificial intelligence issues have been independent research areas. Until recently, cross-disciplinary studies have emerged in these two areas. Although security authentication has been studied in the literature [13]–[15], a new perspective on artificial intelligence-based authentication will help overcome performance limitations and meet the security requirements of new networks. An extreme learning machine-based physical layer authentication approach is designed in [16] to defend against rogue attackers though exploiting the multi-dimensional characteristics of the wireless channel in dynamic networks. Reference [17] proposes a threshold-free physical layer authentication scheme based on machine learning, which improves the detection accuracy without increasing the amount of calculation. To detect the spoofers, [18] presents several adaptive moment estimation algorithms based on deep neural network for lightweight authentication, which can accelerate the training of the authentication model and guarantee extremely low latency. Similarly, neural networks proposed in [19] are used to optimize the encoding and decoding functions, and to learn the trade-off between reliable communication and information secrecy to distinguish eavesdroppers. The authors in [20] give a secure semi-supervised learning scheme based on double learning, which is used to analyze the risk of unlabeled instances according to the classification results. In [21], a learning-based framework for wireless nodes is designed to allow real-time authentication and to distinguish spoofing attackers from the legitimate devices by analyzing their physical features. The deep learning approach is exploited in [22] to identify various attackers, and explore the authentication model in binary and multiclass classification. Recently, a growing number of survey papers study the works that bring artificial intelligence into the field of privacy protection (e.g. [22]–[27]). For example, [23] reviews the potential of applying intelligent adaptive learning approaches in the context of future networks. In addition, with the help of artificial intelligence algorithms, intelligent authentication provisioning can be designed by utilizing channel reciprocity, specific communication link characteristics, and device characteristics [27]–[29]. Along this line, the introduction to deep learning for lightweight physical layer security is presented in [30], dealing with tractable mathematical models. Similarly, in order to guarantee the privacy of wireless communication, a feedforward neural network is proposed in [31]–[33] to classify adversarial attacks. Meanwhile, in the process of data processing, the program divides the trust of the device into different levels and evaluate its behavior.

Although the recent progress of intelligent authentication achieves security enhancement by exploring machine learning, there are still deficiencies in overcoming the above specific challenges. In particular, we point out that additional computational and communication overheads as well as long delays may increase due to prolonged feature extraction and training processes. More importantly, most of the conventional methods still have limitations in statistical properties, which means accurate prediction and authentication framework design is absent. Providing reliable security authentication for wireless networks is the driving force behind our work. Therefore, we focus on envisioning new artificial intelligence-assisted security methods to overcome the challenges described in [34]–[37] and implement secure authentication in wireless multimedia networks.

III. SYSTEM MODEL AND PROBLEM STATEMENT

As shown in Fig. 1, we introduce the system model of our LPLA scheme. We considered many multimedia devices at different locations in a wireless multimedia network scenario. The multimedia nodes are responsible for collecting data and sending it to the data collection center. A malicious device in the network may attempt to eavesdrop and impersonate a legitimate node and then send false multimedia data to the data center for illegal advantages.

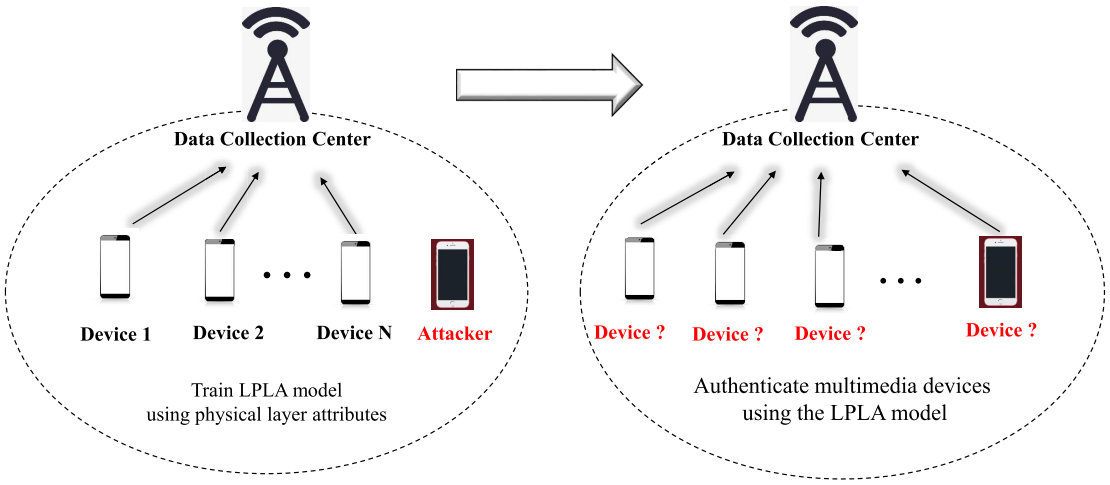

FIGURE 1. The system model of intelligence-based LPLA scheme.

Let $\boldsymbol{h}_x$ denotes the estimated physical layer channel vector, which can be mathematically expressed by

$$\boldsymbol{h}_x = [h_{x,0}, h_{x,1}, h_{x,2}, \cdots, h_{x,M-1}] \quad (1)$$

where M is the number of the sample and the subscript x means "legitimate multimedia device or illegitimate attacker". The LPLA scheme comprises three phases, as shown below.

- *Phase I* : *First of all, the wireless device needs to send its own pilot to the data center to identify the corresponding physical layer attributes through the upper layer identification. In the initialization phase, the LPLA model is trained using training data such as received signal strength (RSS), and corresponding tags. The data center uses multiple physical layer attributes from legitimate devices.*

$$\boldsymbol{H}_{leg}(t) = [\boldsymbol{h}_{leg,0}(t), \boldsymbol{h}_{leg,1}(t), \cdots, \boldsymbol{h}_{leg,N-1}(t)] \quad (2)$$

- *Phase II* : *Then, we use the newly estimated physical layer characteristics to detect legitimate devices and spoofing attackers during the authentication phase.*

$$\boldsymbol{H}_{ill}(t+\tau) = [\boldsymbol{h}_{ill,0}(t+\tau), \cdots, \boldsymbol{h}_{ill,N-1}(t+\tau)] \quad (3)$$

  where τ denotes the time interval between two phases and N represents the number of physical layer attributes.
- *Phase III* : *In the update phase, the training data set is updated with the new physical layer attributes of the legitimate devices, and the LPLA model is retrained to cycle the authentication process.*

$$\boldsymbol{H}_{leg}(t) \leftarrow \boldsymbol{H}_{leg}(t+\tau) \quad (4)$$

The illegitimate device sends signals to the data collection unit and tries to mislead its behavior; however, because of our lightweight intelligent authentication approach, the spoofing attacker will not pass the physical layer authentication, and thus, the data collection center will refuse to receive multimedia data by identifying the abnormal data. In addition to the above security issues, other traditional network security vulnerabilities also apply to our scenarios, such as relay node authentication and impersonation authentication.

IV. ARTIFICIAL INTELLIGENCE BASED LPLA SCHEMES

In our previous research, we introduced the physical layer security authentication algorithm based on the Gaussian mixture model [12]. In this paper, we will further study the new machine learning-based algorithm and propose a lightweight security authentication scheme to meet the high accuracy and low latency requirements of wireless multimedia networks. Among these methods, artificial intelligence contributes to the authentication enhancement not only by learning and mining the physical layer attributes in wireless multimedia networks, but also through providing adaptive retraining for detection model.

A. SECURITY AUTHENTICATION BASED ON MULTIPLE FEATURE EXTRACTION AND SVM

In order to improve the detection accuracy, we first propose a security authentication method based on multiple physical attributes [12] and the support vector machine. To be specific, only when the channel characteristics of the multimedia device are the same as its unique sequence, it will be recognized as a legitimate transmitter by the data collection center.

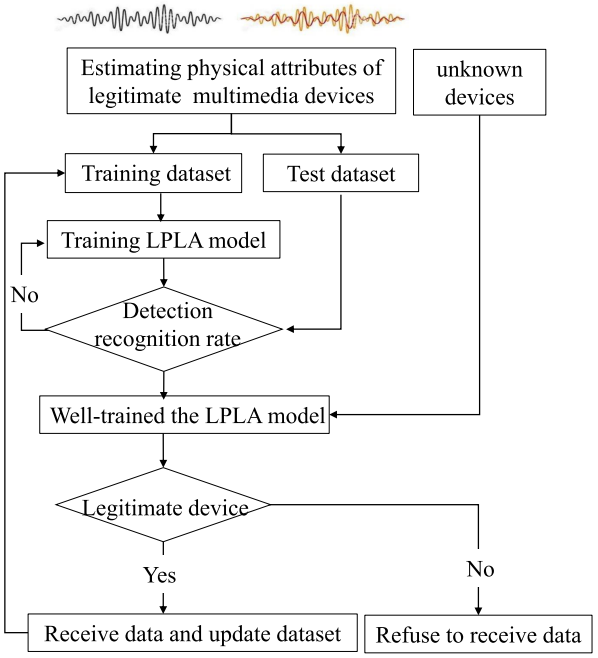

FIGURE 2. The proposed LPLA progress.

Fig. 2 shows the process of the developed LPLA scheme. Firstly, we collected the multi-dimensional channel characteristics that were manually selected. Compared with the one-dimensional feature space, our method improves the detection performance by increasing the uncertainty. Naturally, it is difficult for a spoofing attacker to infer and imitate multi-dimensional physical attributes. Then, a unique binary sequence of different multimedia node is obtained by the data center. In particular, the sequence of features generated by the data center and multimedia device is hidden from any other node due to the unique and unpredictable nature of the wireless communication links used. Therefore, the rogue spoofer can be detected by the trained machine learning-based LPLA model. The same process is performed between each multimedia node and the data collection center using the obtained authenticator. In our scenario, the artificial intelligence algorithm (i.e., support vector machine) improves security by generating an authenticator in the data center, providing sufficient resource space for training. More importantly, the LPLA scheme is designed to take advantage of channel characteristics as an endogenous security mechanism. This eliminates the need for key distribution and management. Because physical layer channels are incredible

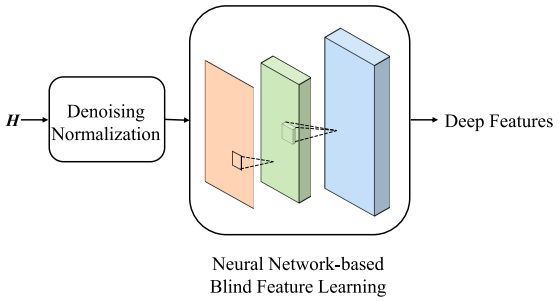

FIGURE 3. The deep learning-based blind feature extraction.

portable, they do not cause additional computational overheads and communication latency. Therefore, the proposed multiple features based authentication scheme is lightweight in the data center of a wireless multimedia network.

B. HOLISTIC APPROACH EXPLOITING BLIND FEATURE EXTRACTION AND DEEP LEARNING

As discussed in the overview, conventional techniques are limited in the choice of channel features. In addition, the authenticator also requires sufficient time to manually select the fixed statistical characteristics, thus leading to a non-adaptive authentication process. In order to achieve fast access authentication, we propose to utilize neural networks to automatically learn deeper blind features. Convolutional neural network can be seen as a black box, where we input the channel estimation matrix $\boldsymbol{H}$ ($N \times 256$) into the black box, as shown in Fig. 3. The convolution operation captures valid blind features from the estimated physical properties. It is worth noting that in our proposed LPLA scheme, the inconsistency between the predicted value of the authentication model and the true label is measured by the softmax loss function. The formulation of softmax loss is given by:

$$L = -\sum_{k=1}^{K} y_k \log s_k \tag{5}$$

where K denotes the number of legitimate multimedia devices, y_k indicates that the corresponding class is set to 1 for the label k, and s_k is the kth value of the output vector s of softmax. More specifically,

$$s_k = \frac{e^{a_k}}{\sum_j^K e^{a_j}} \tag{6}$$

where a_k represents the predicted value belong to the kth multimedia node, which is the output of the final fully connected layer.

The purpose of the convolutional layer is to produce a set of blind features, and the function of each neuron in the network during blind feature learning is beyond our knowledge. A network with more layers can iteratively learn more complex blind features. The mapping operation of two adjacent convolutional layers is as follows:

- input matrix $\boldsymbol{H}^{conv} \in R^{V \times W \times D}$
- the Conv filter $\boldsymbol{F}^{conv} \in R^{V' \times W' \times D \times D''}$
- the output $\boldsymbol{y}^{conv} \in R^{V'' \times W'' \times D''}$

where $V(V'$ or $V'')$ denotes the height, $W(W'$ or $W'')$ is the width, and $D(D'')$ represents the depth. The output of convolutional layer $\boldsymbol{y}^{conv}$ should be calculated as follows

$$\boldsymbol{y}^{conv}_{i'',j'',d''} = \boldsymbol{b}_{d''} + \sum_{i'=1}^{V'} \sum_{j'=1}^{W'} \sum_{d=1}^{D} \boldsymbol{F}^{conv}_{i',j',d,d''} \times \boldsymbol{H}_{S_v(i''-1)+i'-P_v^-, S_w(j''-1)+j'-P_w^-, d} \tag{7}$$

where $\boldsymbol{b}_{d''}$ is the bias, (S_v, S_w) represent the vertical (v) and horizontal (w) input sampling factors, $(P_v^-, P_v^+, P_w^-, P_w^+)$ denote paddings of output in two directions.

The height and the width of the output map are given by

$$V'' = \left\lfloor \frac{V - V' + P_v^- + P_v^+}{S_v} \right\rfloor + 1 \tag{8}$$

$$W'' = \left\lfloor \frac{W - W' + P_w^- + P_w^+}{S_w} \right\rfloor + 1 . \tag{9}$$

In the proposed neural network-based LPLA scheme, we utilize two convolutional layers to learn the efficient bind features. The output data of the convolutional layer will be fed directly into the pooling layer, effectively reducing the dimension of the physical attributes. After two convolution and two pooling operations, the input to the fully-connected layer is the output data of the pooling layer, which is $2 \times 2 \times 128$. We use the fully connected layer as a target classifier in our proposed neural network-based LPLA scheme. The softmax loss is designed to optimize the entire lightweight intelligent authentication scheme during training (details can be found in Eq. (5)).

Like the support vector machine, the proposed neural network is also divided into three steps: the training phase, the authentication phase, and the update retraining phase. During the training phase, the proposed neural network-based LPLA scheme performs a forward propagation and backward propagation iteratively. After the loss tends to converge to a very small value close to zero, the intelligent authentication approach can perform well in authenticating the legitimate multimedia device and rogue attacker. In the authentication phase, we input the newly estimated physical characteristics into a well-trained neural network and give the probability that the received data belongs to different multimedia devices. The predicted value is given by

$$P = \frac{e^{a_k}}{\sum_j^K e^{a_j}} . \tag{10}$$

Notably, the predicted value is calculated by the final fully connected layer. The algorithm authenticates the incoming messages as a legitimate or adversarial multimedia device based on their physical layer characteristics. In our intelligent LPLA scheme, we perform blind feature learning based on convolutional neural network and describe them in the algorithm 1. In the following, we will study and verify the detection performance of LPLA mechanisms.

V. PERFORMANCE EVALUATION

In order to verify the security performance of the presented intelligent authentication approach, two types of

Algorithm 1 Deep Learning-Based LPLA Algorithm

Input: Physical attributes of the i^{th} multimedia device
Output: The authentication result of unknown multimedia device

```
Initialize all connection weights;
Obtain the LPLA model using training dataset;
for new physical attributes do
    compute the probability by the well-trained LPLA model via (10);
    if the transmitter belongs to legitimate devices then
        allow access the data center;
        update the training dataset;
    else
        terminate the connection;
    end if
end for
```

authenticators are selected, including the multiple features-based LPLA method and the neural network based LPLA scheme. Firstly, we implement a LPLA process based on multiple features using some physical layer characteristics and analyze the detection accuracy. Then we demonstrate the superiority of our neural network-based authentication scheme over the conventional approaches, and characterize its accuracy.

First of all, three physical layer features, namely the RSS, the distance between adjacent signals (DAS), and its corresponding pearson correlation coefficient (PCC) are considered in our proposed scheme. Fig. 4 gives the spoofing detection rate of the LPLA scheme based on multiple features. We consider three scenarios: the RSS, the DAS & PCC, and the RSS & DAS & PCC cases. We can observe from Fig. 4 that our LPLA solution relying on the RSS & DAS & PCC has the best security detection performance, while that only relying on the RSS performs worst. The reason for this trend is that the data center can better identify multimedia devices by using multiple features, although spoofer predicts the RSS of legitimate devices. It is also shown in Fig. 4 that there is a small difference between the detection accuracy of the LPLA scheme relying on the DAS & PCC case and that of the RSS & DAS & PCC case; and the detection performance of these multiple features scenarios are better than that of a single-feature case (i.e., RSS). Therefore, an increase in the number of channel features is expected to lead to a higher detection performance in the LPLA scheme.

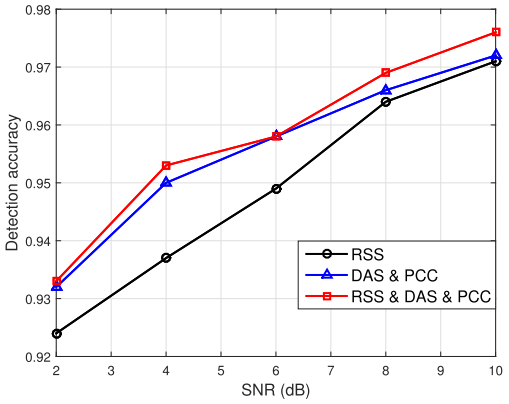

FIGURE 4. Detection performance of the LPLA scheme relying on the RSS, the DAS & PCC, and the RSS & DAS & PCC cases.

Fig. 5 shows the detection accuracy vs. the iteration index for different LPLA schemes. As the number of iterations increases, the detection rate value increases. We can also see from Fig. 5 that the neural network based intelligent LPLA algorithm has the most excellent authentication performance. In other words, deep learning has a better application prospect in extracting physical layer attributes.

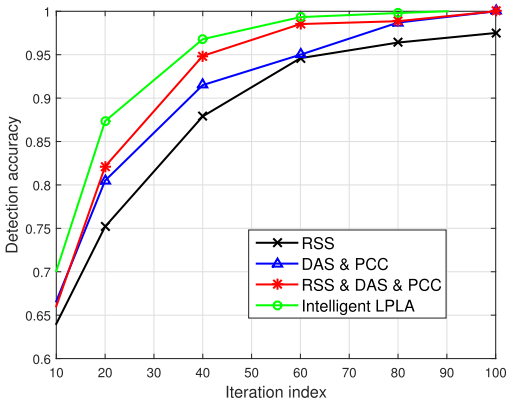

FIGURE 5. Detection performance of LPLA schemes with different physical layer attributes.

Fig. 6 compares the multiple features-based LPLA scheme with the neural network-based intelligent LPLA scheme and analyzes the influence of signal to noise ratio (SNR) on authentication performance. Then we can see from Fig. 6 that as the SNR increases, the detection performance of both schemes is improved. For example, the detection rate of the neural network-based LPLA scheme is 98.6% when the SNR is 12dB. Both Fig. 5 and Fig. 6 confirm that our proposed neural network-based LPLA algorithm has better security performance, because it is more difficult for attackers to imitate the deep features.

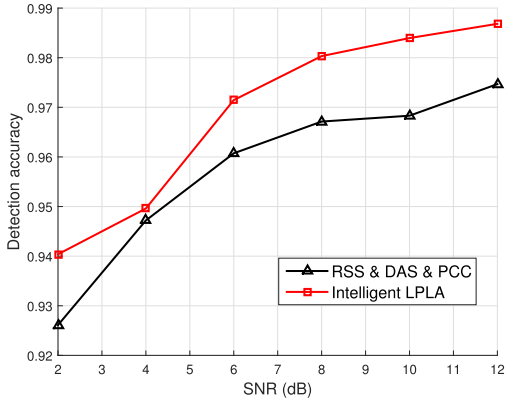

FIGURE 6. Detection performance of different LPLA schemes. (a) the multiple features based LPLA scheme; (b) the neural network based LPLA scheme.

Fig. 7 shows the detection error vs. the iteration index of the presented LPLA schemes. We can observe that detection error rate tends to be a small value when the number of iteration increases from 20 to 100. As mentioned earlier, the neural network-based intelligent LPLA scheme has the best detection performance.

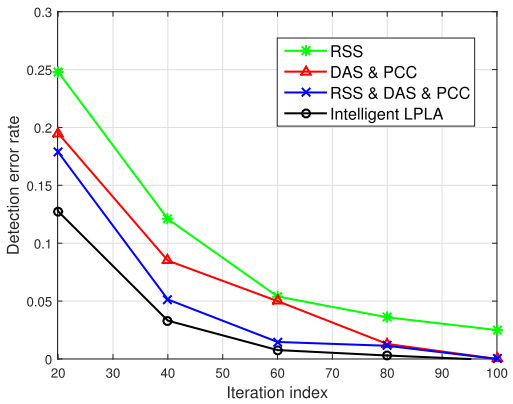

FIGURE 7. Comparison results of our intelligent LPLA scheme with different numbers of physical features.

Table 1 describes the comparison of the artificial intelligence assisted LPLA method with the traditional key-based cryptography method. As can be seen from Table 1, the intelligence-based LPLA scheme can provide 100% security protection because it does not require key transmission, which solves the key leakage problem that may exist in the wireless network. In addition, the intelligence assisted LPLA scheme enables adaptive training and authentication in the time domain. More importantly, physical layer security authentication does not depend on computational complexity and can accurately quantify security. In contrast, key-based cryptography approach requires more time and complexity, which is inefficient for real-time multimedia devices. Therefore, the artificial intelligence-based LPLA scheme achieves fast access authentication and security performance improvement in wireless multimedia networks.

TABLE 1. Comparison results.

Parameter	Intelligence based LPLA scheme	Key based cryptography scheme
Key management and transmission	No	Yes
Channel estimation	Yes	Yes
Feature selection	No	Yes
Pricy amplification	No	Yes
Adaptability	Yes	No
Latency	Low	High
Link	Physical layer	Upper layer
Time complexity of n authentications	O(1)	O(n)

VI. FUTURE PERSPECTIVES

We have shown the challenges of conventional solutions in Section I and discussed some authentication mechanisms for wireless multimedia environments in Section IV. A promising general idea is to study the wireless physical layer attributes and use artificial intelligence to improve detection accuracy. Common to all algorithms that rely on statistical methods is the challenge of feature selection. Especially in an adversarial scenario, the estimated signal preprocessing is an important aspect of these authentication schemes.

Deep learning-driven signal processing is a potential method for selecting physical layer features. Deep learning is an effective way to solve the uncertainty of wireless networks. It provides data-centric channel feature mining and deep feature mapping that can be used for secure authentication modeling. In particular, the deep learning tool provides multiple operators that transform a model-based authentication scheme into a data analytics-centric security technology. Optimally, the security should depend on the data, not the authentication model.

In most cases, the conventional authentication approach works well in an ideal communication environment, but its detection accuracy is significantly reduced when realistic environment interference is introduced. Regardless of the ideal situation, we need to design a suitable adaptive authenticator from a practical perspective. Different assumptions and communication environments make it difficult to improve the adaptability of the authentication model. Thus, solving these open questions is far from trivial-an interesting direction for future research.

VII. CONCLUSION

The artificial intelligence-based security authentication scheme in wireless multimedia networks proposed in this paper has important practical significance. It not only ensures the privacy of communication, but also enables lightweight authentication of multiple multimedia nodes. The physical layer feature-based multimedia device's authentication can achieve better security performance as the dimension of the feature increases. However, its time consumption for manually selecting the appropriate feature will grow as the dimensions of features become larger. Therefore, the multi-feature-based method is applicable to low-level security authentication schemes. Numerical analysis shows that the neural network-based LPLA scheme effectively learns the physical feature parameters, which are usually manually selected in other algorithms. In particular, the neural network based LPLA approach has good detection performance and ultra-short communication latency. It has been found that the artificial intelligence-assisted LPLA method can effectively improve the authentication accuracy and solve the communication latency problem in wireless multimedia network applications.

REFERENCES

[1] D. Wu, Z. Zhang, S. Wu, J. Yang, and R. Wang, "Biologically inspired resource allocation for network slices in 5G-enabled Internet of Things" *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2888543.

[2] P. Zhang, X. Kang, X. Li, Y. Liu, D. Wu, and R. Wang, "Overlapping community deep exploring-based relay selection method toward multi-hop D2D communication," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1357–1360, Oct. 2019.

[3] Z. Zhang, C. Wang, C. Gan, S. Sun, and M. Wang, "Automatic modulation classification using convolutional neural network with features fusion of SPWVD and BJD," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 5, no. 3, pp. 469–478, Sep. 2019.

[4] Z. Li, H. Liu, and R. Wang, "Service benefit aware multi-task assignment strategy for mobile crowd sensing," *Sensors*, vol. 19, no. 12, p. 4666, Oct. 2019.

[5] Z. Li, Y. Jiang, Y. Gao, L. Sang, and D. Yang, "On buffer-constrained throughput of a wireless-powered communication system," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 2, pp. 283–297, Feb. 2019.

[6] D. Wu, H. Shi, H. Wang, R. Wang, and H. Fang, "A feature-based learning system for Internet of Things applications," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1928–1937, Apr. 2019.

[7] P. Zhang, X. Kang, D. Wu, and R. Wang, "High-accuracy entity state prediction method based on deep belief network toward IoT search," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 492–495, Apr. 2019.

[8] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2958–2970, Aug. 2018.

[9] D. Wu, L. Deng, H. Wang, K. Liu, and R. Wang, "Similarity aware safety multimedia data transmission mechanism for Internet of vehicles," *Future Gener. Comput. Syst.*, Vol. 99, pp. 609–623, Oct. 2019.

[10] H. Fang, A. Qi, and X. Wang, "Fast authentication and progressive authorization in large-scale IoT: How to leverage AI for security enhancement?" 2019, *arXiv:1907.12092*. [Online]. Available: https://arxiv.org/abs/1907.12092

[11] M. A. Jan, M. Usman, X. He, and A. U. Rehman, "SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1576–1583, Apr. 2019.

[12] X. Qiu, T. Jiang, S. Wu, and M. Hayes, "Physical layer authentication enhancement using a Gaussian mixture model," *IEEE Access*, vol. 6, pp. 53583–53592, 2018.

[13] N. Xie and C. Chen, "Slope authentication at the physical layer," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1579–1594, Jun. 2018.

[14] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proc. IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.

[15] N. Xie and S. Zhang, "Blind authentication at the physical layer under time-varying fading channels," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1465–1479, Jul. 2018.

[16] N. Wang, T. Jiang, S. Lv, and L. Xiao, "Physical-layer authentication based on extreme learning machine," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1557–1560, Jul. 2017.

[17] J. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R.-F. Liao, and J. Chen, "Threshold-free physical layer authentication based on machine learning for industrial wireless CPS," *IEEE Trans. Ind. Informat.*, to be published.

[18] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, Y. Jiang, F. Xie, and M. Cao, "Deep-learning-based physical layer authentication for industrial wireless sensor networks," *Sensors*, vol. 19, no. 11, p. 2440, May 2019.

[19] R. Fritschek, R. F. Schaefer, and G. Wunder, "Deep learning for the Gaussian wiretap channel," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Mar. 2019, pp. 1–6.

[20] H. Gan, Z. Li, Y. Fan, and Z. Luo, "Dual learning-based safe semi-supervised learning," *IEEE Access*, vol. 6, pp. 2615–2621, 2017.

[21] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using *in-situ* machine learning," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, Feb. 2019.

[22] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[23] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 98–105, Apr. 2017.

[24] A. Ferdowsi and W. Saad, "Deep learning for signal authentication and security in massive Internet-of-Things systems," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1371–1387, Feb. 2019.

[25] H. Ye, G. Y. Li, and B.-H. Juang, "Power of deep learning for channel estimation and signal detection in OFDM systems," *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 114–117, Feb. 2018.

[26] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, Sep. 2018.

[27] Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2595–2621, 4th Quart., 2018.

[28] X. Qiu, T. Jiang, and W. Zou, "Physical layer security in simultaneous wireless information and power transfer networks," in *Proc. 17th Int. Symp. Commun. Inf. Technol. (ISCIT)*, Cairns, QLD, Australia, Sep. 2017, pp. 1–4.

[29] X. Qiu and T. Jiang, "Safeguarding multiuser communication using full-duplex jamming receivers," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, Oct. 2017, pp. 1–5.

[30] T. O'Shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 563–575, Dec. 2017.

[31] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks," May 2019, *arXiv:1905.05137*. [Online]. Available: https://arxiv.org/abs/1905.05137

[32] X. Qiu, T. Jiang, and N. Wang, "Safeguarding multiuser communication using full-duplex jamming and Q-learning algorithm," *IET Commun.*, vol. 12, no. 15, pp. 1805–1811, Sep. 2018.

[33] X. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "Enabling reputation and trust in privacy-preserving mobile sensing," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2777–2790, Dec. 2014.

[34] S. Henningsen, S. Dietzel, and B. Scheuermann, "Misbehavior detection in industrial wireless networks: Challenges and directions," *Mobile Netw. Appl.*, vol. 23, pp. 1330–1336, Oct. 2018.

[35] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, Mar. 2019.

[36] N. Wang, T. Jiang, and Z. Zhou, "Channel sparse representation based authentication for reconciliation of key generation," in *Proc. 16th Int. Symp. Commun. Inf. Technol. (ISCIT)*, Qingdao, China, Sep. 2016, pp. 547–550.

[37] N. Wang, S. Lv, T. Jiang, and G. Zhou, "A novel physical layer spoofing detection based on sparse signal processing," in *Proc. IEEE GlobalSIP*, Orlando, FL, USA, Dec. 2015, pp. 582–585.

XIAOYING QIU (S'18–M'19) received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), in 2019. She is currently a Lecturer with Beijing Information Science and Technology University, Beijing, China. Her main research interests include physical layer security, authentication, and machine learning.

ZHIGUO DU received the B.S. degree in telecommunication engineering from the People's Public Security University of China, in 1999, and the M.E. degree in information and communication system from the Beijing University of Posts and Telecommunications, in 2007. He is currently with the College of Information Technology and Cyber Security, People's Public Security University of China as an Associate Professor. His research interests include vulnerability assessment of security systems and effectiveness evaluation of video surveillance systems.

XUAN SUN received the B.S. degree in mathematics and applied mathematics from the Beijing University of Posts and Telecommunications, Beijing, China, in 2007, and the Ph.D. from the Department of Communication Engineering, Beijing University of Posts and Telecommunications, in 2012. She is currently a Lecturer with Beijing Information Science and Technology University. Her research interests include network security, event flow analysis, and risk detection.