IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 30, 2019, accepted January 27, 2020, date of publication February 3, 2020, date of current version February 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2971260

A Learning Approach for Physical Layer Authentication Using Adaptive Neural Network

XIAOYING QIU[1], (Member, IEEE), JIANMEI DAI[2], (Member, IEEE), AND MONSON HAYES[3], (Life Fellow, IEEE)

[1]School of Information Management, Beijing Information Science and Technology University, Beijing 100192, China
[2]School of Space Information, Space Engineering University, Beijing 101416, China
[3]Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA 22030, USA

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

ABSTRACT In communications, innovative paradigm shifts have emerged in integrating various devices into the network to provide advanced and intelligent services. However, various security threats may occur that may not always be detected using traditional cryptographic techniques. Secure authentication is of paramount importance in modern wireless systems. This paper focusses on robust authentication in a time-varying communication environment where conventional authentication mechanisms are severely limited. We propose an Adaptive Neural Network (ANN) as an intelligent authentication process to improve detection accuracy. Specifically, a Data-Adaptive Matrix (DAM) is designed to track time-varying channel features. By utilizing a convolutional neural network as an intelligent authenticator, the proposed approach integrates deep feature extraction and attack detection, hence, leading to effective physical layer security. To evaluate the system, the ANN is prototyped on a universal software radio peripheral (USRP) and its authentication performance is evaluated in a conference room environment. Experimental results show that the ANN is effective in tackling the challenges of physical layer authentication under interference conditions, and is effective in time-varying environments.

INDEX TERMS Convolutional neural network, physical layer security, intrusion detection, machine learning.

I. INTRODUCTION

Innovative technologies enable physical objects to see, hear, think, accomplish tasks and make intelligent decisions [1]. The Internet of things (IoT) is an emerging wave of technological evolution that involves the communication among a wide network and range of wireless devices in such areas as industrial and home automation, financial enterprises, and medical applications. Densely deployed smart devices are expected to communicate securely and intelligently with minimal human intervention [2]. Given the privacy of the data, secure authentication is especially important before establishing any IoT device connection.

The traditional approach to wireless security is to use digital key-based cryptographic techniques, which is computationally demanding [3]. Since the core function of IoT devices is to ensure the secure exchange of data between billions and even trillions of smart things, computational complexity and latency are important considerations for IoT nodes, which have limited computing power and battery life. Recently, a lightweight security paradigm has been proposed that addressed these issues at the physical layer [4], [5].

A considerable amount of research into the development of algorithms for physical layer authentication has been done over the past several years, along with the development of the technologies necessary to implement these algorithms as well as the supporting mathematical theory and analysis of their performance [6]. For example, Xiao et. al. considered the use of a generalized likelihood ratio test to authentication and to detect a spoofing attacker [7]. However, since their approach requires that the communication channel of the legitimate transmitter and the spoofer be known, their approach is not feasible in a practical setting. Subsequently, the authors proposed a logistic regression technique and were

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

able to remove the assumption of a known channel distribution [8]–[10]. One of the difficult and important challenges in physical layer authentication is how to deal with time varying channels. In [11] a hypothesis test based approach was proposed that considered the spatial variability of propagation.

In order to characterize the properties of a channel, and to allow one to distinguish between a legitimate channel and the channel of a spoofer, a number of different channel features have been considered that include channel phase information [5], [12], [13], received signal strength (RSS) [14]–[16], channel state information [17]–[19], and channel impulse response [20], [21]. Although there has been considerable progress in the development of physical layer authentication methods in time-varying environments, not much work has been done in looking at approaches that are based on deep learning. We have found, along with others, that channel-based authentication methods suffer a tremendous performance degradation in time-varying communication scenarios. Therefore, learning-based authentication methods are essential for improving detection accuracy, and are capable of quickly adapting in time-varying communication environments.

Since channel-based authentication methods use estimates of specific channel characteristics, such as wireless signal variance, strength or even multidimensional features, the effectiveness of these methods rely heavily on the training dataset. In this paper, we propose to use an Adaptive Neural Network (ANN) to detect changes in the channel characteristics and to make a decision on whether or not an attack has occurred. This ANN addresses the challenges of time-varying environments for physical layer authentication. To study the effectiveness of this approach, the system is prototyped on a universal software radio peripheral (USRP) platform and its performance is evaluated in multipath fading wireless environments. Considering the various dynamic interferences, we estimate the signal strength received at different times in a conference room. To achieve this, we first collect the raw measurements of the channel estimates through the USRP. Then, the wavelet filter is used to eliminate high frequency electromagnetic noise. The experiment results show that the ANN approach has higher reliability and robustness in physical layer authentication, especially in time-varying communication environments.

The contributions of this paper are as follows.

- We use physical layer security to deal with spoofing attacks in wireless networks. Since many existing solutions to the problem do not address the requirement of deep channel feature learning in a time-varying environment, this paper addressed the design of a robust adaptive authentication.
- A Data-Adaptive Matrix (DAM) is used to track time-varying physical attributes that is analyzed with a deep Convolutional Neural Network (CNN) for effective detection of rogue attackers. The proposed learning architecture can further search for deep nonlinear features and authenticate intruders in a holistic fusion manner.
- The ANN is prototyped on a USRP platform and its effectiveness is verified in an indoor environment. The experimental results show that the ANN scheme can cope better with current authentication challenges and is superior to existing security authentication algorithms. After training the deep learning-aided model, long-term robustness and convergence tests are performed. Such an analysis has not been available in previous work.

The rest of the paper is organized as follows. We begin with an overview of related work in Section II. Section III presents the system model. This is followed by the overall architecture of the proposed ANN and a detailed design of each component in Section IV. In Section V, we present the experimental setup and performance evaluation. We discuss possible avenues for future research in Section VI and conclude our work in Section VII.

II. BACKGROUND

In the following, we briefly review related work beginning with feature-based authentication strategies, followed by learning-based physical layer authentication.

A. FEATURE-BASED AUTHENTICATION STRATEGIES

The success of physical layer authentication generally depends on the feature representation that is used for the channel characteristics. Feature selection and feature representation is a critical component in physical layer security. In [22], the channel impulse response is used for spoofer detection, whereas the physical layer authentication proposed in [23] uses the time-varying carrier frequency offsets as a radiometric signature. Another well-known channel-based authentication method uses power spectral density estimates to compare subsequent messages [24]. Energy-based authentication in a cellular IoT network is investigated in [25], which utilizes the complex channel gain between the transmitter and the anchor node as a random feature to achieve higher detection accuracy. Extending this result, a multi-antenna identity authentication scheme based on energy ratios was proposed to detect pilot spoofing attacks in [26]. Sparse signal processing and compressed sensing have also been considered in the context of feature extraction as well as physical layer authentication. For example, [27] and [28] considered sparse signal processing from the perspective of feature extraction and in [27] compressed sensing was used for physical layer authentication, achieving a low cost and low complexity with a high security policy. [28] proposed an authentication strategy based on sparse representation to enhance the characteristics of the channel information. In [29]–[31], multi-dimensional characteristics of the radio channel were considered. For example, physical layer authentication in [29] exploits channel signal amplitude and path delay to achieve fast authentication in a high mobility environment. The results show that the inherent two-dimensional

characteristics of channel variations have greater gains in decision rules. Particularly, in [30], a two-dimensional measure space is utilized to preprocess the channel state information. The Euclidean distance and Pearson correlation are used to reduce the impact of channel estimation errors. However, it is worth noting that the device mobility results in low detection accuracy. A similar idea of exploiting multi-dimensional feature space was investigated in [31]. Compared to the one-dimensional feature, the multi-dimensional space enhances the reliability of the inherent link attributes. As a result, the robustness of the physical layer authentication algorithm is greatly improved. Channel characteristic engineering is very important, highlighting the weakness of current authentication schemes. For this reason, a lot of work has been done on channel feature extraction to obtain a data representation that supports physical layer authentication.

B. LEARNING-BASED PHYSICAL LAYER AUTHENTICATION

Learning-based approaches provide many advantages over existing physical layer security and authentication [32], and artificial intelligence algorithms have made their way into intrusion detection and confrontation systems [33]. In many cases, the powerful learning capabilities of intelligent models can compensate for the imperfections in channel parameters estimates. As a result, intelligent physical layer authentication for wireless communications has become a paradigm shift, and machine learning becomes a natural choice with minimal overall cost.

An authentication scheme based on a Gaussian mixture model was proposed in [30] to solve the problem of channel data clustering. Mathematical models based on known physical properties were established. In [34], a support vector machine-based approach was presented to reduce the false alarm probability and in [35] a reinforcement learning-based authentication algorithm was proposed that enabled the receiver to choose the optimal test threshold. While the analysis performed provided valuable insight, the proposed algorithm required a lot of memory to store records. There has been a lot of research works on deep learning, for example, a Bi-layered Parallel Training Convolutional Neural Networks (BPT-CNN) has been proposed in a distributed computing environment [36], [37]. The work in [38] proposed a deep learning scheme for intelligent video surveillance systems with edge computing. Authors in [39], [40] designed a new artificial intelligence enabled security authentication by using channel reciprocity. To achieve security enhancement, game theory has been used to analyze the interactions between autonomous devices with their own goals. For example, cognitive radio networks studied in [41] formulate a zero-sum jamming game. The game theoretic research of physical layer authentication introduced in [35], [42] investigated the double-threat attacker, and a learning-based algorithm was developed to approach to the Nash equilibrium strategy. Inspired by the successful application of learning algorithms in the field of physical layer security, deep neural networks have also been applied to anti-spoofing countermeasures. In [43], a deep learning classifier was used to authenticate the features produced by filter banks.

Although the above methods achieve improved performance by exploring machine learning algorithms, they are still shortcomings in overcoming communication overhead. Most existing neural networks are data driven and hindered by strong assumptions on the rogue spoofers and are still limited when dealing with time-varying environments. Hence, we focus on designing a new artificial intelligence-assisted physical layer security scheme to achieve adaptive authentication.

III. SYSTEM MODEL

The threat model studied in this paper is illustrated in Fig. 1, where Alice transmits signals to Bob in the presence of an active attacker, Eve, who intends to eavesdrop and impersonate Alice, and then disrupt the communication to gain illegal advantage. It is assumed that this wireless network has no privacy. Therefore, Eve can eavesdrop on the message Alice sent to Bob. Assume that the legitimate transceiver agrees to a shared secret key authentication method that allows Bob to identify Alice. Bob's goal is then to verify the received message.

The physical layer signatures of wireless networks have three characteristics that make physical layer authentication a difficult problem. The first is that the wireless network environment changes dynamically over time. This means that any authentication scheme must be able to adapt to time-varying channel characteristics. Second, because the environment is full of reflections and diffractions, the physical attributes become uncorrelated in space, time and frequency. Therefore, each location is unique in terms of channel properties. Third, since communication transmission exists in a random fading environment, imperfect estimation and incomplete measurement of wireless signals are inevitable. These lead to unpredictable variations in authentication systems.

Physical layer authentication in our threat model consists of two time slots, as described below.

A. THE FIRST TIME SLOT

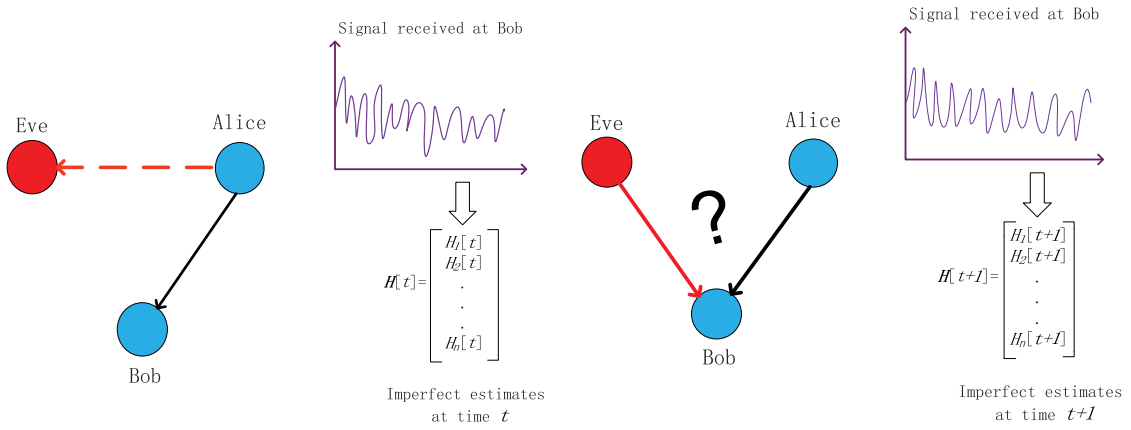
Alice broadcasts legitimate signals to Bob, while Eve is an eavesdropper. As the signal is received from Alice, Bob estimates the physical attributes of the legitimate channel,

$$\boldsymbol{H}_A(t) = [H_{A,1}(t), H_{A,2}(t), \cdots, H_{A,n}(t)]^T \tag{1}$$

where A indicates that the signal is from Alice and n represents the number of estimated vectors.

B. THE SECOND TIME SLOT

Given that Eve has eavesdropped on the signal sent by Alice at time t, she may transmit spoofing messages to Bob by masquerading Alice's media access control (MAC) address. Bob must authenticate the transmission that he receives at



(a) Threat model at t time slot (b) Threat model at $t+1$ time slot

FIGURE 1. A threat model in the wireless network. In the first period, Alice sends useful signals to Bob, while Eve is an eavesdropper. Then Eve is a malicious transmitter who masquerades as Alice to intercept communication between legitimate nodes. Bob needs to authenticate the received message.

time $t+1$

$$\boldsymbol{H}(t+1) = [H_1(t+1), H_2(t+1), \cdots, H_n(t+1)]^T \ , \quad (2)$$

and determine whether or not it is coming from Alice. The receiver may then compare $\boldsymbol{H}(t+1)$ to $\boldsymbol{H}_A(t)$, and if they are close, then the message is likely to have come from Alice. We may define H_0 as the null hypothesis that the signal is from Alice (i.e., the estimate is $\boldsymbol{H}_A$), and H_1 the hypothesis that the transmitter is Eve and perform the hypothesis test:

$$H_0 : |\boldsymbol{H}_A(t) - \boldsymbol{H}(t+1)| \leq \gamma \quad (3)$$

$$H_1 : |\boldsymbol{H}_A(t) - \boldsymbol{H}(t+1)| > \gamma \quad (4)$$

where γ is the test threshold that controls the detection accuracy.

The problem with this approach is that the underlying physical channel is time-varying and imperfectly estimated. Therefore, these static channel characteristics are limited in their ability to correctly authenticate the transmission. It is for this reason that the use of a data matrix that captures the recent history of the channel is proposed. A sequence of data matrices is then used to train a CNN to learn the physical attributes of the channel, and then be used to authenticate the transmission or to detect a spoofer. Since a USRP platform is used in our experiments, we focus on the RSS as shown in Fig. 2.

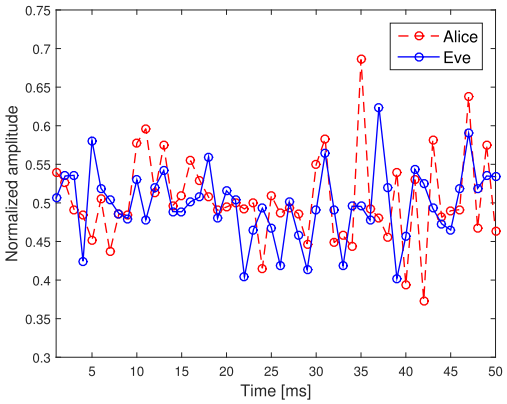


FIGURE 2. RSS of the different transmitters for 50 milliseconds in the conference room.

IV. INTELLIGENT AUTHENTICATION SYSTEM

The overall architecture of the ANN-based physical layer authentication system is shown in Fig. 3. Since the physical layer attribute measurements are imperfect estimates and are noisy, the data to be authenticated is preprocessed with a wavelet-based noise filter. After preprocessing the raw data, a data-adaptive matrix is created that is used as the input to the ANN. This matrix consists of a sequence of RSS vectors that captures the time-varying properties of the channel. After training, the ANN is used to detect changes in the channel that indicate the presence of an intruder. In the following, we begin with a discussion of the data-adaptive matrix.

A. DATA-ADAPTIVE FEATURE MATRIX

The traditional approach to authentication considers only the stationary physical layer attributes, ignoring the time-varying nature of the channel. Naturally, the performance of a physical layer authentication system is largely affected by the changing propagation and interference conditions. To deal with this, attention is focussed on an innovative approach for adaptively adjusting the authentication system as described below.

Let the estimated channel vector at time t be denoted by $H_{A,r} = (h_1, h_2, \ldots, h_{256})^T$, where h is a sample of the pilot signal. Given r estimated channel vectors, $H_{A,r}H_{A,r-1}, \ldots, H_{A,1}$, these vectors are used to form a data-adaptive matrix $\boldsymbol{H}$. When a new estimated channel vector, H_{test}, is received it is appended to the end of the matrix $\boldsymbol{H}$. This augmented data-adaptive matrix is then input to the

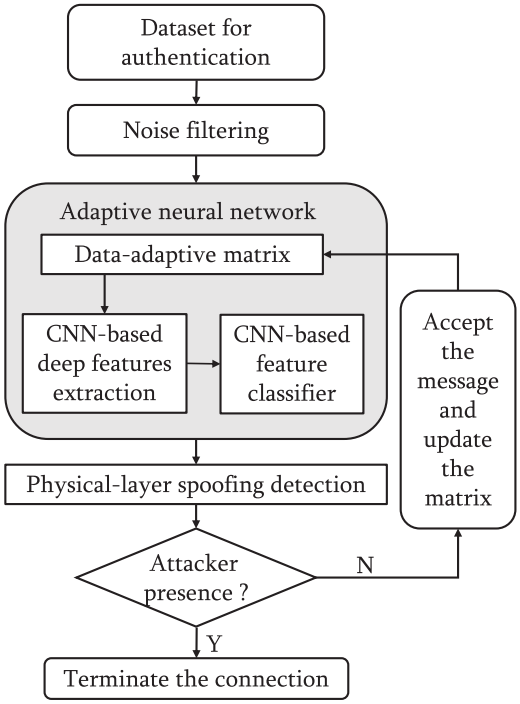


FIGURE 3. System architecture of ANN.

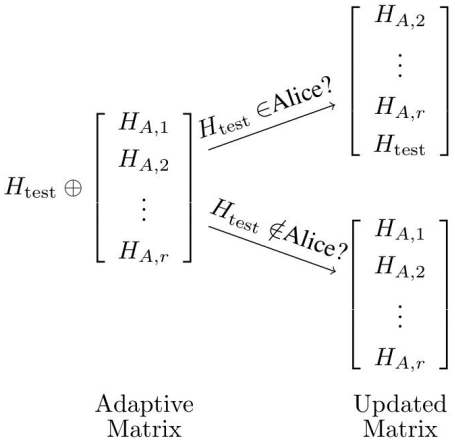


FIGURE 4. Construction and time-evolution of the data-adaptive matrix $\boldsymbol{H}$.

CNN where a decision is made as to whether or not H_{test} comes from Alice. If it does, then a new data-adaptive matrix is formed by discarding $H_{A,1}$. Otherwise, H_{test} is discarded. This process is shown in Fig. 4. Note that the adaptive matrix is time-varying property and it can be used to model the relationship between a series of continuous physical layer estimates. The next section focuses on learning the deep characteristics of physical layer attributes and detecting malicious spoofers.

B. AUTO-EXTRACTOR/CLASSIFIER WITH A CNN

Inspired by the successes that CNNs have had in a wide variety of applications, here a CNN is used to learn the features of the legitimate channel and perform spoofer detection. The CNN consists of two convolution layers and two pooling layers that are used to learn the feature representation of the channel, followed by a fully connected final layer that performs the final classification. The data that is used as the input to the CNN is the data-adaptive matrix $\boldsymbol{H}$ consisting of eight rows of RSS data of length 256. Therefore, $\boldsymbol{H}$ is an 8×256 matrix that consists of eight consecutive RSS vectors. However, the rows of the data matrix are first reshaped into 16×16 arrays, which results in a $16 \times 16 \times 8$ tensor that is used as the input to the CNN. The first convolution layer uses a 2×2 kernel with a stride of 2 and a ReLU activation function. Four feature maps are produced, resulting in an output tensor of size $8 \times 8 \times 32$. This is followed by a max-pooling layer with a kernel size of 2×2 and a stride of 2, which produces an output tensor of size $4 \times 4 \times 32$. The second convolution and pooling layers have the same structure as the first, resulting in output tensors of size $2 \times 2 \times 128$ and $1 \times 1 \times 128$, respectively. The final layer is fully-connected with a single output using a logistic activation function,

$$\phi(a) = \frac{1}{1 + e^{-a}} . \tag{5}$$

The final output represents the probability that the new channel attribute belongs to Alice.

TABLE 1. CNN structure.

Description	Input Size	Output Size
Convolution 1	$16 \times 16 \times 8$	$8 \times 8 \times 32$
Pooling 1	$8 \times 8 \times 32$	$4 \times 4 \times 32$
Convolution 2	$4 \times 4 \times 32$	$2 \times 2 \times 128$
Pooling 1	$2 \times 2 \times 128$	$1 \times 1 \times 128$
Fully Connected	$1 \times 1 \times 128$	$1 \times 1 \times 1$

C. ANN TRAINING

To train the ANN we use the back propagation algorithm using cross-entropy for the cost function. Since each convolution layer has a 2×2 kernel and produces eight feature maps, the total number of weights in the CNN is thirty-two plus eight biases, for a total of 40. Therefore, the structure is simple and does not require the storage of a large number of parameters. However, since the raw data input vector is only of length 256, then the number of parameters is relatively large by comparison. Therefore, since there is sampling noise and uncertainties in the estimated channel attributes, it is possible that there will be overfitting. To reduce the possibility of overfitting and to prevent stagnation in the back propagation algorithm, dropout is used during training [44]. Dropout is a technique that randomly removes a unit from the

Algorithm 1 ANN-Based Authentication Algorithm

Require: step size N_q, and all connection weights;
Repeat (for each episode)
obtain the estimated channel vector;
construct the data-adaptive matrix $\boldsymbol{H}$;
train ANN model using adaptive matrix;
for new physical attributes **do**
    obtain new test dataset based on $\boldsymbol{H}_{test}$;
    get the predictive value with trained ANN;
    if $H_0 = 1$ **then**
        accept this message;
        update $\boldsymbol{H}_A(k) \leftarrow \boldsymbol{H}_A(k+1)$;
    else
        keep $\boldsymbol{H}_A(k)$;
        terminate the connection;
    end if
end for
End Repeat

network during one pass of the back propagation algorithm by setting its weights equal to zero. The probability that a neuron is removed is defined by a hyperparameter p. Dropout has the effect of producing an ensemble of ''thinned'' networks that, in turn, reduces overfitting. The effect of predicting the average of all these thinned networks can be approximated by simply using a single unthinned network with the weights multiplied by $(1 - p)$, the probability that the neuron is not dropped. The optimal dropout rate for the weights at the input layer is typically close to zero and, in our experiments, it was found that the best dropout rate was $p = 0$ for all layers, indicating that overfitting is not a significant problem. Once the CNN has been trained, it is used to make a decision between a legitimate transmitter and a rogue attacker. Pseudo-code for the ANN-based authentication approach is illustrated in Algorithm 1.

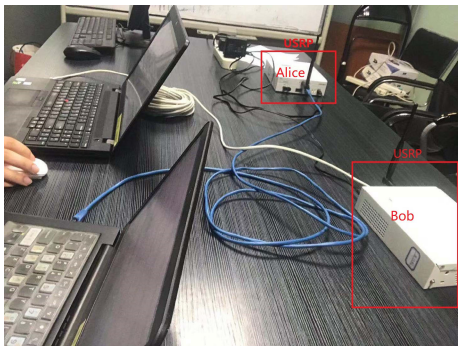
In the following section, we describe the experimental set-up and performance of our system.

V. EXPERIMENTS AND DISCUSSION

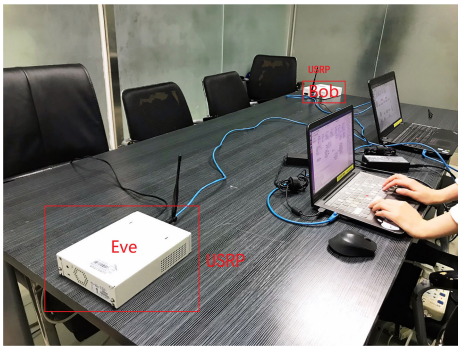
In this section, the prototype implementation of the ANN is presented. Then, the experimental setup and the performance of the proposed approach to authentication is given. For testing, raw data is input to the ANN and the probability that the received channel data belongs to the legitimate transmitter Alice is determined.

A. IMPLEMENTATION

To evaluate the performance of the adaptive authentication system, USRP devices were used in a 6m×4m conference room. A single antenna USRP device was used as the transmitter (TX) to send wireless signals to a USRP receiver (RX). Fig. 5 and Fig. 6 show the conference room and the layout for data collection. To collect data packets, single antenna USRP transceivers were used to operate using the IEEE



(a) Conference room: Alice-to-Bob



(b) Conference room: Eve-to-Bob

FIGURE 5. Experimental areas.

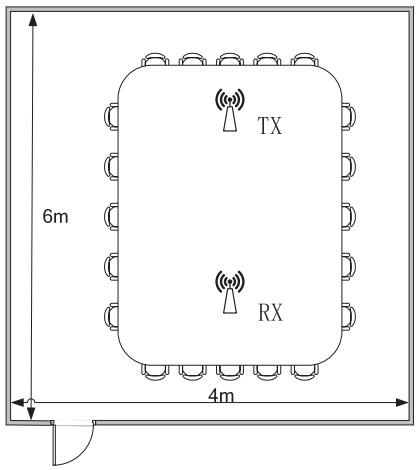


FIGURE 6. Floor plan of the conference room.

802.11a/g standard, working at 2.4 GHz with a bandwidth of 20 MHz. Since there is interference within the conference room, the transmitter Bob and receiver Alice were placed a distance of one meter away from each other and the distance between Eve and Bob was set to 2m. A computer was used to collect and store the physical layer estimates. For training and testing, 2000 sets of data for each TX-RX combination was collected. More specifically, two different channel classes were in the ANN dataset, one consisting of 2000 records for the channel from Alice to Bob and the other consisting of 2000 records for the channel from Eve to Bob.

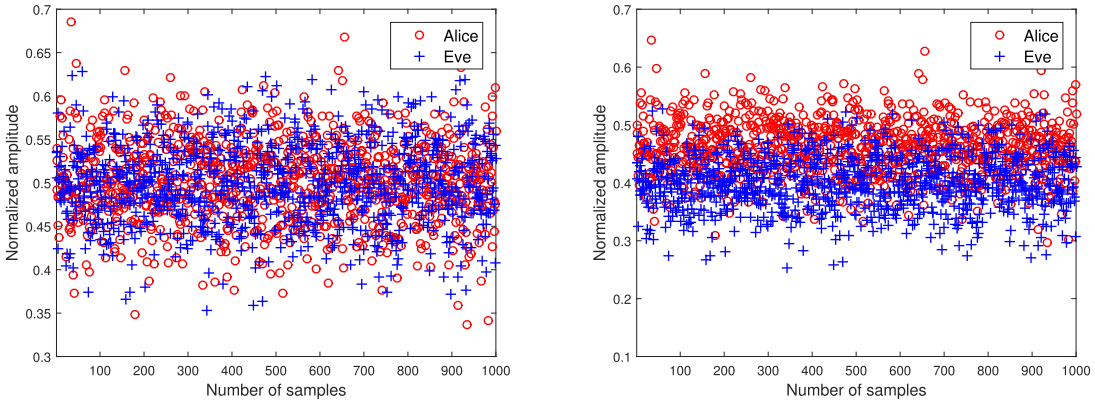


FIGURE 7. (a) The average of the RSS data vectors $H_{a,i}$ for Alice and Eve and (b) The average of the adaptive data matrices H when H_{test} comes from Alice and when it comes from Eve.

Each channel record contained 256 samples, so in total there were 4000×256 RSS data samples. For training, 1000 channel records are selected randomly for each channel, and the remaining were used for testing as shown in the table below.

B. PERFORMANCE EVALUATION

In this section, simulation results are presented that show the performance of the ANN authentication approach. First, the ANN is implemented using the adaptive data matrix and CNN for feature representation and classification. Then, the convergence of the back propagation algorithm for ANN training is presented, and the authentication detection rate is given. We set the threshold $\gamma = 50\%$. The performance metrics used to evaluate the spoofing detection are:

- *Loss Value*: The error between the predicted value and the true value.
- *Detection Rate*: The probability that a spoofer is detected.

Then, the performance of the ANN approach is compared to other authentication methods. Finally, the ANN approach is compared to key-based cryptographic methods for authentication in terms of complexity, latency and other properties of importance.

1) PERFORMANCE OF ANN

Given 1000 RSS data records from two different channels, one for Alice and one for Eve, the effectiveness of using the average of the RSS vectors compared to the data adaptive matrix approach for distinguishing between the two channels is shown in Fig. 7. Specifically, shown in Fig. 7(a) are the normalized average RSS amplitudes for each of the 1000 data records. It is clear that there are no obvious predictable differences between the average RSS amplitudes for Alice's channel and Eve's channel. Fig. 7(b), on the other hand, shows the average of the normalized RSS amplitude of the data-adaptive matrices $\boldsymbol{H}$ when H_{test} comes from Alice and when it comes from Eve. Unlike the case for the normalized

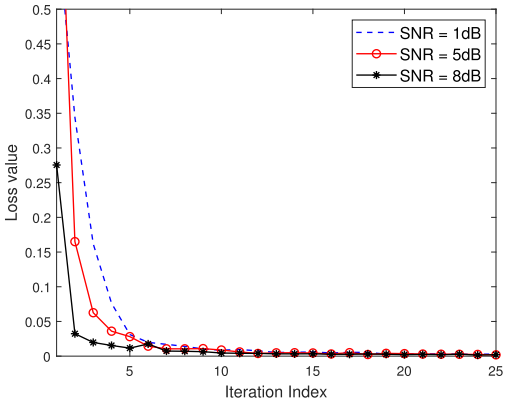


FIGURE 8. The loss function during training of the CNN that is used for channel classification.

average RSS data matrix H, there is now an obvious detectable difference between the two channels. Therefore, it is clear that the data-adaptive matrix is more effective in capturing the differences between the two channels. Although the data adaptive channel matrix has improved the difference between the legitimate and illegitimate channels, in a real communication environment the RSS vectors are not necessarily the most effective features to use to detect a channel transmission from a spoofer. Therefore, we consider using a deep CNN to learn the features in the physical layer attributes that are best for authentication.

Fig. 8 shows the cross-entropy loss function versus the iteration index during training of the ANN using the back propagation algorithm for SNRs of 1 dB, 5 dB, and 8 dB. Note that the loss is close to zero after fewer than ten iterations for all SNRs, but the convergence is faster for higher SNRs. The reason for this, obviously, is that the channel data estimated using the USRP platform is more accurate when the SNR is high, which implies that the quality of wireless communication environment determines the training accuracy of the intelligent authentication model. In the

TABLE 2. Splitting of the dataset.

Subsets	Training	Testing
Alice	1000×256	1000×256
Eve	1000×256	1000×256

TABLE 3. The performance comparison between the proposed intelligent authentication scheme and the existing algorithms.

SNR	Detection Rate (%)			
	SVM	GMM	CNN	ANN
4dB	91.95	95.01	89.16	**95.89**
6dB	97.50	95.99	97.99	**100.00**
8dB	98.01	96.56	98.96	**100.00**
10dB	98.88	98.01	99.75	**100.00**

wireless communication environment, when using the USRP transceiver to verify the effectiveness of the authentication algorithm, there are many uncontrollable interference factors, such as channel estimation error, time-varying environments and surrounding wireless signal interference. Given the performance on the training data to discriminate between two channels as illustrated in Fig. 8, with the loss function almost zero, it is apparent that a CNN is able to effectively extract the relevant features and perform physical layer authentication. However, in order to verify this, it is necessary to look at the detection rate on real data, and then compare the performance of ANN with other approaches.

Given a data set of 2000 RSS vectors, this data set is split into a training set and a test set as shown in Table 2. After training, the features that are learned are used to detect channel changes in the test set, which indicate the presence of a spoofer. Shown in Table 4 is the detection rate (in percent) of spoofer attacks for channel SNRs that vary from 4 dB to 10 dB. Note that the detection rate is 100% for SNRs that are 6 dB and above, and for 4 dB it is 95.89%. For SNRs that are 4 dB and below, the performance deteriorates significantly. However, it is important to put these numbers in the context of how state-of-the-art spoofing detection approaches perform. The authentication accuracy of three different machine learning methods are shown in Table 4. Note that ANN outperforms the GMM approach [30] when the SNR is 4 dB or higher. Finally, to see the effectiveness of the data adaptive matrix, also shown in Table 4 are the detection rates using a CNN without the data adaptive matrix, i.e., using the average RSS vectors. What we observe is that there is an improvement of between 4% and 6% using the data adaptive matrix. Thus, we see that the ANN method obtains better spoofing detection performance compared with

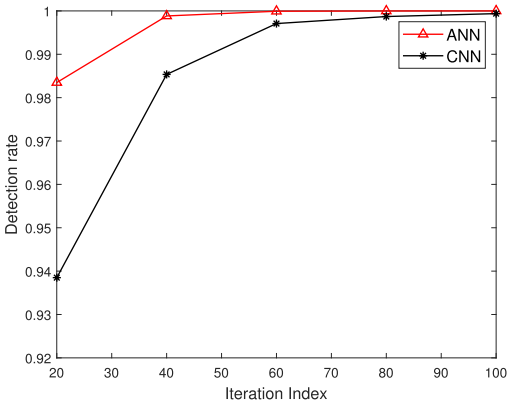


FIGURE 9. Detection performance comparison results, SNR= 8dB.

GMM and SVM and better than using CNN alone without the data adaptive matrix. This is because by utilizing an adaptive feature matrix, the proposed ANN scheme can further explore time-varying physical attributes, i.e., the adaptive feature matrix introduced in Section IV-A. More importantly, compared with other machine learning approaches, ANN is an end-to-end system that can learn deeper channel characteristics between different channels and detect spoofer simultaneously. However, existing authentication methods typically use two separate processes, namely, first extracting channel features and then classifying different transmitters using a learning model to detect spoofing attackers. Since the task is to prototype ANN on a USRP platform and verify the effectiveness of the algorithm in an indoor conference room, the surrounding interference noise has a greater impact than the ideal data simulation. In this case, if some valid channel characteristic information is lost during the channel estimation process, it is irreversible if we still intend to use these missing parts to train the authentication model. To solve this problem, the ANN scheme integrates these two processes to ensure the fusion of feature extraction and classification.

Fig. 9 compares what happens when the intelligent authentication process uses both DAM and CNN to the case when the CNN is used with the RSS vectors. What is shown is that the detection performance of the ANN that uses DAM and CNN is better than the CNN method, indicating that the ANN can recalibrate the time-varying physical attributes. Another interesting observation is that ANN-based method performs well in detecting spoofing attackers, even if the performance is sensitive to our real experimental environment. It is also shown in Fig. 8 that the DAM-based intelligent ANN algorithm has the best authentication performance. In other words, deep learning has a better application prospect in extracting physical layer attributes.

Fig. 10 shows the loss function versus the iteration index in two different cases, namely the line-of-sight (LOS) and non-line-of-sight (NLOS) cases. It can be seen that the ANN authenticator has better training performance in the LOS case. This, however, is as expected since ANN relies only on correlations between different reconstruction matrices.

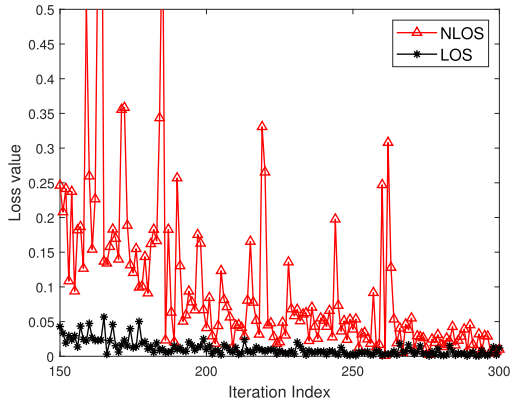


FIGURE 10. Training performance of ANN in LOS and NLOS scenarios.

TABLE 4. Comparison results.

	Authentication Method	
Parameter	ANN	Key-based
Key management and transmission	No	Yes
Manual feature selection	No	Yes
Privacy amplification	No	Yes
Dynamic	Yes	No
Latency	Low	High
Complexity for n times of authentication	O(1)	O(n)

In addition, interference from other WiFi signals could lead to performance degradation. In fact, although the proposed ANN authentication scheme is verified in a complex time-varying conference room, the detection rate is still accurate.

2) COMPLEXITY ANALYSIS

Shown in Table 4 is a comparison of ANN-based authentication with traditional key-based cryptography approaches. As seen in the table, ANN does not require key transmission, which avoids problems with possible key leakage in wireless networks. In addition, the ANN method 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. By contrast, the key-based cryptography approach requires more time and complexity, which is problematic for sensor devices. Therefore, the ANN-based authenticator achieves fast access authentication and security performance improvement in wireless networks.

VI. FUTURE RESEARCH DIRECTIONS

A number of physical layer authentication mechanisms for wireless communication systems were presented in Section II and in Section V the advantages of learning-based authentication scheme were presented. A promising idea is to leverage artificial intelligence algorithms to intelligently model the authentication process to improve detection accuracy. Common to all methods that rely on simple static characteristics is the challenge of time-varying communication links. Especially in the scenario of using USRP, channel variation propagation and imperfect estimation are important factors in the design of physical layer authentication schemes.

Although ANN uses the USRP platform already deployed in a conference room for spoofing authentication, there are still some challenges that need to be addressed. For example, our system has not yet been able to authenticate devices in moving scenarios. Authenticating moving devices has always been a more challenging issue than authenticating static devices. Besides, the USRP devices deployed in the experiment are single-antenna, we envision a multi-antenna intelligent authentication model for future research.

VII. CONCLUSION

This paper presents ANN, an Adaptive-Convolutional Neural Network for physical layer authentication. Since static physical characteristics are not sufficient in a time-varying communication environment, a data-adaptive matrix is used for signal preprocessing. To ensure reliable performance under imperfect channel estimation, an intelligent authentication algorithm named "ANN" is proposed that can establish an automatic interaction between deep learning representation and spoofing authentication. The ANN scheme was evaluated in a conference room environment and the convergence and detection accuracy were demonstrated over time. ANN is a robust authentication approach that adapts to complex time-varying environments, and is superior to other learning-based methods. With these advantages, we believe that ANN is promising in physical layer authentication and other related applications.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[2] P. Hao, X. Wang, and W. Shen, "A collaborative PHY-aided technique for end-to-end IoT device authentication," *IEEE Access*, vol. 6, pp. 42279–42293, 2018.

[3] 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.

[4] 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.

[5] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[6] H. Taha and E. Alsusa, "Secret key exchange and authentication via randomized spatial modulation and phase shifting," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2165–2177, Mar. 2018.

[7] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5948–5956, Dec. 2009.

[8] X. Wan, L. Xiao, Q. Li, and Z. Han, "FHY-layer authentication with multiple landmarks with reduced communication overhead," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–6.
[9] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676–1687, Mar. 2018.
[10] M. Jaggi, "Revisiting Frank-Wolfe: Projection-free sparse convex optimization," in *Proc. Int. Conf. Mach. Learn. (ICML)*, Atlanta, GA, USA, Jun. 2013, pp. 427–435.
[11] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.
[12] X. Wu and Z. Yang, "Physical-layer authentication for multi-carrier transmission," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 74–77, Jan. 2015.
[13] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, 1st Quart., 2016.
[14] Y. Chen, J. Yang, 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, pp. 2418–2434, Jun. 2010.
[15] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-based secret key generation in underwater acoustic networks: Advantages, challenges, and performance improvements," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 32–38, Feb. 2016.
[16] J. Huang and T. Jiang, "Dynamic secret key generation exploiting Ultra-wideband wireless channel characteristics," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, New Orleans, LA, USA, Mar. 2015, pp. 1701–1706.
[17] T.-Y. Liu, P.-H. Lin, S.-C. Lin, Y.-W.-P. Hong, and E. A. Jorswieck, "To avoid or not to avoid CSI leakage in physical layer secret communication systems," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 19–25, Dec. 2015.
[18] H. Liu, Y. Wang, J. Liu, J. Yang, and Y. Chen, "Practical user authentication leveraging channel state information (CSI)," in *Proc. ACM Symp. Inf., Comput. Commun. Secur.*, Kyoto, Japan, 2014, pp. 389–400.
[19] L. Wang, C. Jiang, L. Kuang, S. Wu, H. Huang, and Y. Qian, "High-efficient resource allocation in data relay satellite systems with users behavior coordination," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12072–12085, Dec. 2018.
[20] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.
[21] F. J. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Budapest, Hungary, Jun. 2013, pp. 4724–4728.
[22] A. Mahmood, W. Aman, M. O. Iqbal, M. M. U. Rahman, and Q. H. Abbasi, "Channel impulse response-based distributed physical layer authentication," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, Jun. 2017, pp. 1–5.
[23] 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, pp. 1658–1667, May 2014.
[24] J. K. Tugnait, "Spectrum-based comparison of multivariate complex random signals of unequal lengths," in *Proc. 51st Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, USA, Oct. 2017, pp. 757–761.
[25] G. Caparra, M. Centenaro, N. Laurenti, S. Tomasin, and L. Vangelista, "Energy-based anchor node selection for IoT physical layer authentication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.
[26] Q. Xiong, Y.-C. Liang, K. Hung Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.
[27] N. Wang, T. Jiang, W. Li, and S. Lv, "Physical-layer security in Internet of Things based on compressed sensing and frequency selection," *IET Commun.*, vol. 11, no. 9, pp. 1431–1437, Jun. 2017.
[28] N. Wang, W. Li, T. Jiang, and S. Lv, "Physical layer spoofing detection based on sparse signal processing and fuzzy recognition," *IET Signal Process.*, vol. 11, no. 5, pp. 640–646, Jul. 2017.
[29] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171–4182, Jun. 2016.
[30] 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.
[31] 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.
[32] 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.
[33] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.
[34] C. Pei, N. Zhang, X. S. Shen, and J. W. Mark, "Channel-based physical layer authentication," in *Proc. IEEE Global Commun. Conf.*, Austin, TX, USA, Dec. 2014, pp. 4114–4119.
[35] L. Xiao, T. Chen, G. Han, W. Zhuang, and L. Sun, "Game theoretic study on channel-based authentication in MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7474–7484, Aug. 2017.
[36] J. Chen, K. Li, K. Bilal, X. Zhou, K. Li, and P. S. Yu, "A bi-layered parallel training architecture for large-scale convolutional neural networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 5, pp. 965–976, May 2019.
[37] C. Zhang, G. Sun, Z. Fang, P. Zhou, P. Pan, and J. Cong, "Caffeine: Towards uniformed representation and acceleration for deep convolutional neural networks," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 38, no. 11, pp. 2072–2085, Nov. 2019.
[38] J. Chen, K. Li, Q. Deng, K. Li, and P. S. Yu, "Distributed deep learning model for intelligent video surveillance systems with edge computing," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/tii.2019.2909473.
[39] S. Gu, T. Lillicrap, I. Sutskever, and S. Levine, "Continuous deep q-learning with model-based acceleration," in *Proc. Int. Conf. Mach. Learn.*, New York, NY, USA, 2016, pp. 2829–2838.
[40] 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
[41] C. Chen, M. Song, C. Xin, and J. Backens, "A game-theoretical anti-jamming scheme for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 22–27, May 2013.
[42] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.
[43] H. Yu, Z.-H. Tan, Z. Ma, R. Martin, and J. Guo, "Spoofing detection in automatic speaker verification systems using DNN classifiers and dynamic acoustic features," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 10, pp. 4633–4644, Oct. 2018.
[44] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: A simple way to prevent neural networks from overfitting," *J. Mach. Learn. Res.*, vol. 15, no. 1, pp. 1929–1958, 2014.

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

JIANMEI DAI (Member, IEEE) received the B.E. degree in communication engineering and the M.S. degree in communication and information systems from the Academy of Equipment, Beijing, China, in 2004 and 2007, respectively. He is currently a Lecturer with Space Engineering University, Beijing. His research interests include optimization theory and its applications in wireless video transmission and wireless networks.

MONSON HAYES (Life Fellow, IEEE) received the B.A. degree in physics from the University of California at Berkeley, and the M.S.E.E. and D.Sc. degrees in electrical engineering and computer science from M.I.T. He was a Professor of electrical and computer engineering with the Georgia Institute of Technology until 2011, and served as an Associate Chair with the School of ECE, Georgia Tech, and as an Associate Director of Georgia Tech Savannah. From 2011 until 2014, he was a Distinguished Foreign Professor with Chung-Ang University, Seoul, South Korea, with the Graduate School of Advanced Imaging Science, Multimedia, and Film. Since 2014, he has been a Professor and the Chair of the Department of Electrical and Computer Engineering, George Mason University, Fairfax, Virginia. He is currently a Professor Emeritus with Georgia Tech. He has published over 200 articles, and is the author of the textbook *Statistical Digital Signal Processing and Modeling* (John Wiley and Sons, 1996). He has served the Signal Processing Society for the IEEE in numerous positions, including a General Chairman for ICASSP 1996, ICIP 2006, and ICASSP 2018.