IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 14, 2018, accepted November 28, 2018, date of publication December 4, 2018, date of current version December 27, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2884672

Security in Fog Computing: A Novel Technique to Tackle an Impersonation Attack

SHANSHAN TU[1,2], (Member, IEEE), MUHAMMAD WAQAS[3], (Student Member, IEEE), SADAQAT UR REHMAN[3], (Student Member, IEEE), MUHAMMAD AAMIR[4], OBAID UR REHMAN[5], JIANBIAO ZHANG[1], AND CHIN-CHEN CHANG[6], (Fellow, IEEE)

[1]Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China
[2]Beijing Key Laboratory of Trusted Computing, Beijing 100124, China
[3]Department of Electronic Engineering, Tsinghua University, Beijing 100084, China
[4]School of Engineering, Edith Cowan University, Joondalup, WA 6027, Australia
[5]Department of Electrical Engineering, Sarhad University of Science and Information Technology, Peshawar 25000, Pakistan
[6]Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan

Corresponding author: Muhammad Waqas (wa-j15@mails.tsinghua.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61801008, in part by the National Key Research and Development Program of China under Grant 2018YFB0803600, in part by the Beijing National Natural Science Foundation under Grant L172049, and in part by the Beijing Science and Technology Planning Project under Grant Z171100004717001.

ABSTRACT Fog computing is an encouraging technology in the coming generation to pipeline the breach between cloud data centers and Internet of Things (IoT) devices. Fog computing is not a counterfeit for cloud computing but a persuasive counterpart. It also accredits by utilizing the edge of the network while still rendering the possibility to interact with the cloud. Nevertheless, the features of fog computing are encountering novel security challenges. The security of end users and/or fog nodes brings a major dilemma in the implementation of real life scenario. Although there are several works investigated in the security challenges, physical layer security (PLS) in fog computing is not investigated in the above. The distinctive and evolving IoT applications necessitate new security regulations, models, and evaluations disseminated at the network edge. Notwithstanding, the achievement of the current cryptographic solutions in the customary way, many aspects, i.e., system imperfections, hacking skills, and augmented attack, has upheld the inexorableness of the detection techniques. Hence, we investigate PLS that exploits the properties of channel between end user and fog node to detect the impersonation attack in fog computing network. Moreover, it is also challenging to achieve the accurate channel constraints between end user and fog node. Therefore, we propose Q-learning algorithm to attain the optimum value of test threshold in the impersonation attack. The performance of the propose scheme validates and guarantees to detect the impersonation attack accurately in fog computing networks.

INDEX TERMS Fog computing, physical layer security, reinforcement learning, impersonation attack.

I. INTRODUCTION

In the last decade, due to the exponential growth of mobile internet traffic, the attractiveness of mobile devices has been directing the remarkable development in wireless communication and networking [1]. Particularly the revolutions in small cells based heterogeneous networks, massive multiple input and multiple output (MIMO) and millimeter (mm)-Wave communications cater users gigabit wireless access in next generation [2], [3]. Therefore, the remote cloud data centers have high processing power and large memory storage that enables low processing mobile devices to run their respective computing services. However, cloud computing has certain limitations. For instance, the data generation and consumption can be occurred at diverse applications, users' locations, interaction time and response time. For instance, video calls, voice and online gaming are highly affected by users' movement and locations [4]. This leads to higher latency, processing and storage requirements, and such problems varies across applications. In this new era, the users' requirement of lower latency, lower processing and storage may not be suitable for applications relying on cloud computing due to static condition of cloud, and long distance between cloud-servers and end-users. Additionally, the data execution of different applications does not take user mobility

into consideration in cloud computing [5]–[8]. Therefore, cloud computing is inadequate for a broad range of egressing mobile applications. It is necessary that the data processing of an application can take place at a geographically distributed data centers. This conducted to the egression of novel research arena called fog computing and networking [9], [10].

However, fog computing networks become vulnerable to impersonation attack due to the exposed nature of wireless behavior between fog node and end users. In impersonation attack, nodes (fog nodes & end users) can claim to become an alternative user/node by utilizing a forged character i.e., media access control address (MAC-A). Therefore, an impersonation attack would acquire the illegitimate benefits, and accomplish man-in-the-middle attacks as well as denial-of-service (DoS) attacks [11], [12]. To cope with the problem, PLS technique is considered a promising methodology to cover the security needs of wireless physical layer [15]. PLS techniques leverage physical layer properties of the wireless communication links to cope with the impersonation attack. The properties of physical layer (i.e., received signal strength (RSSs), received signal strength indicators (RSSIs), channel frequency response (CFR), and channel state information (CSI)), are taken into consideration as the identifications of wireless channels between nodes to perceive the impersonation attack [13]–[15].

In the reinforcement learning methods, for instance Q-learning, the user would get the optimal schemes in dynamic setting without being conscious of system's details. In addition, the end users are not static in real life, and the channel between the end user and fog server is continuously changing due to the movement of end users or for node. Hence, in real life scenario, the environment between end user and fog node is not static but dynamic. Therefore, we apply Q-learning algorithm to detect the impersonation attack from the dynamic environment. The PLS is proposed by exploiting the channel states of the wireless packets between nodes. Therefore, the channel responses are difficult to predict and easily tempered by the attackers. Here, a hypothesis test relates the CFR of the data with similar MAC-A. This determines the test value threshold grounded on the reinforcement learning in dynamic wireless communication. It is deprived of knowing the complete information of the channel parameter i.e., the channel time variations. The accuracy of the PLS impersonation attack is depending on the value of test threshold in hypothesis test, which is achieved at the receiver end. This is a perplexing for a receiver node to indicate an appropriate threshold value without perceptive of the accurate values of channel parameters against non-legitimate nodes. These non-legitimate nodes can submissively prefer their attack probabilities to fleece and impersonate efficiently. In addition, the optimal value of the test threshold in hypothesis test of the Q-learning would accomplished by trial and error to exploit the long-term effectiveness.

Although fog computing can play a central role in delivering a rich portfolio of services more effectively and efficiently to end users, yet it is imposed by diverse security challenges [16], [17]. Hence, the security issues of IoT in fog computing are tackled in different ways. For instance, Ni *et al.* [18] proposed secure service authentication scheme for networking slicing and for computing for IoT services. Additionally, the authors also introduce the negotiation of session keys among end users, local fog nodes and IoT services to guarantee secure access of service data. In another article, Fu *et al.* [19]suggested a retrieval features tree to support secure data retrieval and an index encryption scheme. The encryption scheme is based on the secure k-nearest neighbor (kNN) algorithm to support privacy-preserving data search. A securable and verifiable outsourcing scheme is investigated in [20] to compute the matrix inverse in a server to secure user data. The authors proposed a secret key generation based on chaotic system for matrix encryption and decryption to protect input and output data privacy. Alrawais *et al.* [21] proposed key exchange protocol based on cipher-text policy attribute based encryption (CP-ABE). The authors combine CP-ABE and digital signature technique to achieve confidentiality, authentication, verifiability and access control. Hu *et al.* [22] proposed authentication and session key agreement scheme, data encryption scheme and data integrity checking scheme to solve the issues of confidentiality, integrity, and availability in the processes of face identification and face resolution using fog computing in IoTs.

It can be seen that most of the existing works did not consider the physical layer security in fog computing network. Researchers tried to secure the network security by conventional techniques of cryptography, and did not pay attention towards communication security between end users and fog servers/nodes. They do not exploits the properties of physical layer security, and the randomness or variation in the channel between their physical connectivity. No work to date however has explicitly considered the PLS technique in fog computing networks. Against the above research background, we pay attention to the impersonation attack in fog computing through physical layer security. The impersonation attack is tackle in with reinforcement learning. The research on the security issue of fog computing is still in its early stage. Therefore, in this article, we take a closer look at the security issue of fog computing. Moreover, it is the first work to investigate the physical layer security (PLS) in fog computing through reinforcement learning. The main contributions of this work are as complies.

- We propose physical layer security (PLS) to tackle the impersonation attack. The PLS exploits the CSI of the wireless packets in order to perceive the impersonation attack. We formulate the zero-sum game between an attacker and the receiver in a static environment.
- We propose reinforcement learning technique i.e., Q-learning in order to attain an optimal value of the test threshold of the dynamic environment for the hypothesis test. The hypothesis test is based on the channel state information (CSI), and find out diverse factors such as, the average time, false alarm rate (FAR), miss detection

rate (MDR) and average error rate (AER). We investigate that the Q-learning in a dynamic environment improves the impersonation detection attack and the accuracy of the receiver by learning from the dynamic environment.

The rest of the paper is organized as follows. After the introduction in Section I, we illustrate the system overview, model and problem formulation in Section II. The reinforcement learning technique for impersonation attack detection is also described in Section II. The performance evaluation of our propose method is presented in Section III. Finally, Section IV depicts the discussion section, and Section V concludes the paper.

II. SYSTEM OVERVIEW, MODEL AND PROBLEM FORMULATION

We consider a wireless communication links between fog node and end users in fog computing networks. The network consists of $N = \{1, 2, \cdots, n\}, \forall n \in N$ receivers and $M = \{1, 2, \cdots, m\}, \forall m \in M$ transmitters as shown in Fig. 1. The network consists of $I = \{1, 2, \cdots, i\}, \forall i \in I$ of legitimate nodes and $F = \{1, 2, \cdots, f\}, \forall f \in F$ non-legitimate nodes that impersonate the authentic node with fake MAC-A. The non-legitimate node can either fog node, who want to impersonate towards the end user or vice versa. Hence, the total transmitters in the network is $M = (I \cup F)$. However, we differentiate them with different notations in order to differentiate the legitimate node from non-legitimate node. The MAC-A of mth transmitter is represented by $\gamma_m \in \Gamma$, $\forall m \in M$, where Γ is the set of all MAC-A. The illegitimate node can send a fake MAC-A in a time slot with probability i.e., $p_j \in [0, 1]$. The receiver n approximates the CSI related with the packet, once a packet is received. Particularly, the pilots of the packet can use for the channel response estimation of the linked transmitter. However, it is positioned at the frequency f_o, along with the bandwidth B. The receiver

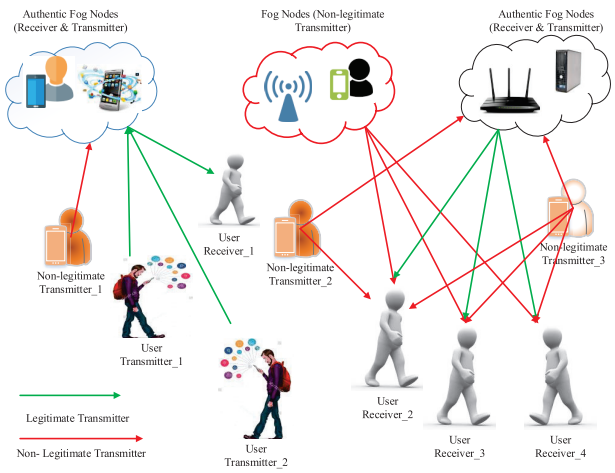


FIGURE 1. General overview of impersonation attack in fog computing.

$n \in N$ samples the CSI for each packet in the communication link between nodes. Therefore, the channel vector of the tth packet from the mth transmitter is represented by $\alpha_\gamma^t = \left[\alpha_{\gamma,x}^t\right]_{1\le x\le X}$. We also denoted the channel record of the tth packet from the mth transmitter by $\beta_\gamma^t = \left[\beta_{\gamma,x}^t\right]_{1\le x\le X}$. In this discussion, the α_γ^t and β_γ^t are the channel vector and channel record, respectively, by the xth tone of the tth packet from the transmitter i.e., $M = (I \cup F)$.[1]

Next, we perform the hypothesis test to investigate the authentication of the packet i.e., a packet with the channel vector α_γ^t is certainly driven by the legitimate transmitter. Therefore, we denote the MAC-A of the node that transmits a packet with channel vector α_γ^t by $\mathcal{U}(\alpha_\gamma^t)$. The hypothesis $\mathcal{H}_\circ$ implies that the packet of the MAC-A is transmitted by the legitimate node. Alternatively, the hypothesis $\mathcal{H}_\star$ is the test of non-legitimate transmitter i.e., a packet is transmitted by non-legitimate transmitter. Therefore, the impersonation detection is grounded on the following hypothesis test and is specified by

$$\mathcal{H}_\circ : \mathcal{U}(\alpha_\gamma^t) \ge \Gamma, \tag{1}$$

$$\mathcal{H}_\star : \mathcal{U}(\alpha_\gamma^t) \ne \Gamma. \tag{2}$$

In PLS, the channel state information is unique, therefore, the receiver can authenticate the tth packed based on the channel state information (CSI). Thus, on the basis of CSI, if the channel vector i.e., $\mathcal{U}(\alpha_\gamma^t)$ and the channel record $\mathcal{U}(\beta_\gamma^t)$ are identical, then the packet sent by the transmitter will be considered as legitimate packet. Conversely, the packet is sent from non-legitimate node. On this point, we can formulate the statistic of the hypothesis test in the impersonation attack. The statistic is denoted by

$$\mathcal{S}\left((\alpha_\gamma^t), (\beta_\gamma^t)\right) = \frac{\left\|(\alpha_\gamma^t) - (\beta_\gamma^t)\right\|^2}{\left\|(\beta_\gamma^t)\right\|^2}. \tag{3}$$

In (3), $\|\cdot\|$ is the Frobenius norm, and $\mathcal{S}$ is the normalized Euclidean distance between α_γ^t and β_γ^t, respectively. We fix the test threshold i.e., λ. Therefore, we can illustrate that if $\mathcal{S}\left((\alpha_\gamma^t), (\beta_\gamma^t)\right) < \lambda$, the receiver node $n \in N$ accepts the $\mathcal{H}_\circ$, otherwise, the receiver accept $\mathcal{H}_\star$. Consequently, the hypothesis tests for impersonation attack in PLS is given by

$$\mathcal{S}\left((\alpha_\gamma^t), (\beta_\gamma^t)\right) < \lambda \implies \mathcal{H}_\circ, \tag{4}$$

or

$$\mathcal{S}\left((\alpha_\gamma^t), (\beta_\gamma^t)\right) > \lambda \implies \mathcal{H}_\star. \tag{5}$$

According to (3), $\mathcal{S}\left((\alpha_\gamma^t), (\beta_\gamma^t)\right) \ge 0$. In result, $\lambda \ge 0$. Therefore, in the next step, we define the probability of FAR and MDR. The FAR is the probability that a legitimate node sent an authentic packet, but the receiver notice it as non-legitimate packet. Here, it is denoted by $\mathcal{P}_\mathcal{A}$ and is given by

$$\mathcal{P}_\mathcal{A} = \mathcal{P}_\mathcal{R}\left(\mathcal{H}_\star | \mathcal{H}_\circ\right). \tag{6}$$

[1]Note that, the transmitter can be either legitimate node, represented by $i \in I$ or it can be also be impersonated node (non-legitimate node) i.e., $f \in F$ who are pretending to be a legitimate node (impersonation attack)

Here, $\mathcal{P}_{\mathcal{R}}(\cdot|\cdot)$ is to be conditional probability. We have also the possibility of MDR, and it is the probability that a non-legitimate packet is considered as legitimate packet by the receiver. Thus, we denote the MDR by $\mathcal{P}_{\mathcal{B}}$, and is given by

$$\mathcal{P}_{\mathcal{B}} = \mathcal{P}_{\mathcal{R}}(\mathcal{H}_{\circ}|\mathcal{H}_{\star}). \tag{7}$$

However, the probability for a receiver to consent an authentic packet from (6) is set by

$$\mathcal{P}_{\mathcal{R}}(\mathcal{H}_{\circ}|\mathcal{H}_{\circ}) = 1 - \mathcal{P}_{\mathcal{A}}. \tag{8}$$

Similarly, the probability for a receiver to discard a non-legitimate packet from (7) is specified by

$$\mathcal{P}_{\mathcal{R}}(\mathcal{H}_{\star}|\mathcal{H}_{\star}) = 1 - \mathcal{P}_{\mathcal{B}}. \tag{9}$$

The detection accuracy of the PLS authentication in (4) and (5) depends on the value of test threshold i.e., λ. It is assumed that by increasing the test threshold λ, the MDR of the non-legitimate node increases. On the other side, the small value of λ consequently increases the FAR. Therefore, the most important factor for the receiver is to select the test threshold value (λ) to avoid impersonation attack. However, it is also assumed that the receiver pertains the higher layer authentication (HLA) to process the packets that get permitted by the PLS authentication. It is considered in our work that the only packets are accepted if and only if both the PLS authentication and HLA accept the packet. It is assumed that the channel record β_{γ}^{t} is updated once a packet is transmitted from the transmitter M, and is acknowledged by HLA, i.e., $\beta_{\gamma}^{t} \leftarrow \alpha_{\gamma}^{t}$. Conversely, it will updated as $\beta_{\gamma}^{t} \leftarrow \beta_{\gamma}^{t-1}$.

The impersonation detection method in (4) and (5) can be formulated initially by zero-sum game, and thus to find the utility function. In zero sum game, there are $\mathcal{F}$ non-legitimate nodes and $\mathcal{N}$ receivers [23]. The receivers apply the PLS authentication to detect the impersonation attack while each unauthentic node sends packets by exploiting the MAC-A of an authentic transmitter. Each receiver selects the threshold test value $\lambda \in [0, \infty)$ in the hypothesis test to perceive the impersonation attack. The non-legitimate nodes select their delude frequency and is denoted by $p_j \in [0, 1]$, $1 \leq j \leq \mathcal{F}$. The set of all non-legitimate packets of the non-legitimate nodes are denoted by $\mathbb{Y} = \left[p_j\right]_{1 \leq j \leq \mathcal{F}}$. It is considered that non-legitimate nodes can cooperate each other to send the delude packets without collisions with $\sum_{j=1}^{\mathcal{F}} p_j \leq 1$. However, it is assumed that only one non-legitimate node attacks as an impersonated node in a time slot. Therefore, the probability for the receiver to attain a delude packet is written as $\sum_{j=1}^{\mathcal{F}} p_j$.

The accuracy of the impersonation detection method is highly depended on the utility of the receiver. The gain of the receiver to accept the legitimate packet is denoted by $\mathcal{G}_1$, whereas, the gain of the receiver to reject the non-legitimate packet is denoted by $\mathcal{G}_0$. Similarly, the cost for receiver to deceptively discard the packet of the legitimate node is denoted by $\mathcal{C}_1$, whereas, the cost for a receiver to deceptively accept a delude packet from non-legitimate node is denoted by $\mathcal{C}_0$. At this stage, we define the Bayesian risk [24]–[26] of the impersonation detection under a prior distribution of the impersonation attack is denoted by $\mathbb{E}(\lambda, \mathbb{Y})$, and is given by

$$\begin{aligned}\mathbb{E}(\lambda, \mathbb{Y}) = \big(\mathcal{G}_1(1 - \mathcal{P}_{\mathcal{A}}(\lambda)) - \mathcal{C}_1\mathcal{P}_{\mathcal{A}}(\lambda)\big)\big(1 - \sum_{j=1}^{\mathcal{F}} p_j\big) \\ + \big(\mathcal{G}_0(1 - \mathcal{P}_{\mathcal{B}}(\lambda)) - \mathcal{C}_0\mathcal{P}_{\mathcal{B}}(\lambda)\big)\big(\sum_{j=1}^{\mathcal{F}} p_j\big).\end{aligned} \tag{10}$$

In (10), the first term i.e., $\big(\mathcal{G}_1(1-\mathcal{P}_{\mathcal{A}}(\lambda)) - \mathcal{C}_1\mathcal{P}_{\mathcal{A}}(\lambda)\big)\big(1 - \sum_{j=1}^{\mathcal{F}} p_j\big)$ corresponds to the gain from a legitimate packet, whereas the second term i.e., $\big(\mathcal{G}_0(1 - \mathcal{P}_{\mathcal{B}}(\lambda)) - \mathcal{C}_0\mathcal{P}_{\mathcal{B}}(\lambda)\big)\big(\sum_{j=1}^{\mathcal{F}} p_j\big)$ is the gain under an impersonation attack i.e., non-legitimate node. The utility of the non-legitimate node, and a receiver in the zero-sum game is denoted by $\mathcal{U}_{\mathcal{F}}(\lambda, \mathbb{Y})$, and $\mathcal{U}_{\mathcal{N}}(\lambda, \mathbb{Y})$, respectively. As defined the Bayesian risk in (10), the utilities of the non-legitimate node and a receiver are given by

$$\begin{aligned}\mathcal{U}_{\mathcal{N}}(\lambda, \mathbb{Y}) &= -\mathcal{U}_{\mathcal{F}}(\lambda, \mathbb{Y}) = \mathbb{E}(\lambda, \mathbb{Y}) \\ &= \big(\mathcal{G}_0 - \mathcal{G}_1\big)\sum_{j-1}^{\mathcal{F}} p_i - \big(\mathcal{G}_0 + \mathcal{C}_0\big)\mathcal{P}_B(\lambda)\sum_{j=1}^{\mathcal{F}} p_j \\ &\quad - \big(\mathcal{G}_1 + \mathcal{C}_1\big)\mathcal{P}_{\mathcal{A}}(\lambda)\big(1 - \sum_{j=1}^{\mathcal{F}}(p_j)\big) + \mathcal{G}_1.\end{aligned} \tag{11}$$

The PLS impersonation detection is based on the frequency responses of the channel with a single attacker that is denoted by $\mathbb{G} = \big[\{n, f\}, \{\lambda, p\}, \{\mathcal{U}_{\mathcal{N}}, \mathcal{U}_{\mathcal{F}}\}\big]$. It consists of receiver n, $\forall n \in \mathcal{N}$, and an attacker f, $\forall f \in \mathcal{F}$. Therefore, the receiver selects its test threshold value $\lambda \in [0, \infty)$. The attackers also establish their attack frequency $p \in [0, 1]$. Thus, the utilities of the receiver and attacker are given by (11). The utilities function in (11) is based on static PLS. However, for more practical scenario, the environment between end users and fog nodes is changing at every instant due to mobility, and thus we achieve the incomplete information of the channel state. In result, we present reinforcement learning in the next section to uncover the optimal scheme with an incomplete information of the channel state in dynamic environment.

The Q-learning is the reinforcement learning algorithm that can be utilized to seek out the optimum stratagem with inadequate information in a dynamic environment [27], [28]. It is stated that the receivers are oblivious of the channel model and delude frequencies in a dynamic radio environment. Therefore, the optimum test threshold would be attained by the receiver's end through error and trail in the impersonation detection. Generally, it is assumed that optimal legitimation threshold value λ^* will decrease with the number of attack encounters. In Q-learning algorithm, each agent is learnt to attain the optimal strategy. The receivers build the hypothesis test to evaluate the transmitter for each $\mathcal{T}$ packets acknowledged in the time slot for impersonation detection

with Q-learning. The test threshold i.e., λ is selected from $L+1$ stages, i.e., $\lambda \in \{l/L\}_{0\leq l\leq L}$. The states perceived by the receiver's end at time τ, and this is represented by s_τ, comprises FAR as well as MDR at time $\tau-1$. This is represented by $s_\tau = [\mathcal{P}_{\mathcal{A}}^{t-1}, \mathcal{P}_{\mathcal{B}}^{t-1}] \in \mathbb{S}$, where the $\mathbb{S}$ is the set of all the states those detected by the receivers. The error rates are quantized into $L+1$ levels, i.e., $\mathcal{P}_{\mathcal{A}}, \mathcal{P}_{\mathcal{B}}, \in \{l/L\}_{0\leq l\leq L}$. These receivers select their action λ_τ on the basis of state s_τ to maximize the expected utility sum that is denoted by Π_τ, and is given by

$$\Pi_\tau = \sum_{t=(\tau-1)\mathcal{T}+1}^{\tau\mathcal{T}} \mathcal{U}_{\mathcal{N}}^{t}.(\lambda, \mathbb{Y}). \tag{12}$$

In (12), the $\mathcal{U}_{\mathcal{N}}^{t}$ is the immediate utility function represented in (11). The receiver indicates the suboptimal actions with a small probability ϵ on the basis of ϵ-greedy policy. However, the preference of the utility that is maximized by the optimal actions is $1-\epsilon$. Hence, the probability is given by

$$\Upsilon_r(\lambda) = \begin{cases} 1-\epsilon, & \lambda = \lambda^*, \\ \epsilon/L, \lambda \in \{l/L\}_{\lambda\leq l\leq L}, & \lambda \neq \lambda^*. \end{cases} \tag{13}$$

In Q-learning, the impersonation detection depend upon the learning rate, i.e., $\mu \in (0, 1]$. This implies the weight of the present Q-function i.e., $\mathcal{Q}(s_\tau, \lambda_\tau)$. The discount factor signifies the improbability on the rewards impending, which is expressed by $\delta \in (0, 1]$. The value of the state s is the maximum value of the $\mathcal{Q}$-function, and is represented by $\mathcal{V}(s)$. Consequently, the receivers update its $\mathcal{Q}$-function as follows:

$$\mathcal{Q}(s_\tau, \lambda_\tau) \leftarrow (1-\mu)\mathcal{Q}(s_\tau, \lambda_\tau) + \mu(\Pi_\tau + \delta\mathcal{V}(s_\tau + 1)), \tag{14}$$

$$\mathcal{V}(s_\tau) \leftarrow \max_{\lambda\in\{l/L\}_{0\leq l\leq L}} \mathcal{Q}(s_\tau, \lambda). \tag{15}$$

The optimal value of the test threshold, λ^* is given by

$$\lambda^* = \arg \max_{\lambda\in\{l/L\}_{0\leq l\leq L}} \mathcal{Q}(s_\tau, \lambda). \tag{16}$$

In order to obtain an optimal action, and maximizes the utility, we summarise the impersonation attack detection discussion in Algorithm 1.

Algorithm 1 Algorithm for Impersonation Detection

Step # I Initialization:
Compute ϵ, μ, δ, $\mathcal{Q}(s, \lambda)$, $\mathcal{V}(s) = 0$, $\forall\lambda \in \{l/L\}_{0\leq l\leq L}$.
Step # II: Current State:
while $\tau = 1, 2, 3, \cdots$ **do**
  Observe the current state s_τ
  Choose the test threshold value λ_τ;
  for $t = 1$ *to* $\mathcal{T}$ **do**
    Notice MAC-A $\gamma_m \in \Gamma$
    Extract α_γ^t and β_γ^t
    Calculate $\mathcal{S}\big((\alpha_\gamma^t), (\beta_\gamma^t)\big)$, Ref. to (3)
    if $\mathcal{S}\big((\alpha_\gamma^t), (\beta_\gamma^t)\big) \leq \lambda_\tau$ **then**
      Pass tth packet for HLA
      $\beta_\gamma^t \leftarrow \alpha_\gamma^t$
      Accept the tth packet
      else;
      Reject the tth packet;
    end
  end
  Step # III: Next State:
  Observe $s_{\tau+1}$
  Observe Π_τ
  Update $\mathcal{Q}(s_\tau, \lambda_\tau)$ Ref. to (14)
  Update $\mathcal{V}(s_\tau)$ Ref. to (15)
end

III. PERFORMANCE EVALUATION

In this section, we perform our simulation results to evaluate the impersonation attack. In the performance evaluation, we consider randomly scattered nodes in 500×500 m^2 square area. All the channels gains are rendered accordingly to the conventional distribution of $\xi(0, 1)$. The center frequency is set to be $f_0 = 2.4$ GHz, along with $\mathcal{G}_0 = 9$, $\mathcal{G}_1 = 6$, $\mathcal{C}_0 = 4$, $\mathcal{C}_1 = 2$, $p = 0.3$, $\mu = 0.6$, and $\epsilon = 0.6$. Moreover, as there is no existing work done for fog computing security based on PLS impersonation attack, therefore, we compared our results with the fixed threshold as a zero-sum game. Hence, fixed threshold value is considered as a benchmark for impersonation attack in our analysis.

In our first experiment, we calculated the average time to detect the impersonation attack. This is based on the time taken by the receivers to detect the impersonated bits/node. It is obvious that as the number of bits/node is increasing, the average time for the receiver to detect the legitimate and non-legitimate bits/node are also increasing. However, the average time taken by Q-learning is lower and stabilizes as compared to fixed threshold value. Thus, it is concluded from Fig. 2 that the performance of Q-learning is almost 47% lower than the fixed threshold value. We also calculate the probability of reliability to detect the impersonation attack based on bits/node. As the number of transmitter increases, more and more bits are required to detect by the receiver for authentication. Therefore, the reliability of the receiver to detect the impersonation attack decreases as shown in Fig. 3.

The FAR and MDR of the hypothesis test is also calculated for Q-learning and is given by [29]

$$\mathcal{P}_{\mathcal{A}}(\lambda) = 1 - F_{x_{2M}^2}\Big(\frac{2\lambda\rho}{2\rho^2 + b\rho\sigma^2}\Big). \tag{17}$$

$$\mathcal{P}_{\mathcal{B}}(\lambda) = F_{x_{2M}^2}\Big(\frac{2\lambda\rho}{2\rho^2 + (1+k)\rho\sigma^2}\Big). \tag{18}$$

In (17) & (18), $F_{x_{2M}^2}(\cdot)$ is the cumulative distribution function with the degree of freedom $2M$. The receiver observes the average power gain of the authentic transmitter by σ^2. ρ is the signal-to-interference plus noise ratio (SINR) of the legitimate packet of an authentic transmitter. The relative change in the channel's gain is b, owing the dynamic variations in the environment. k is measured as the ratio

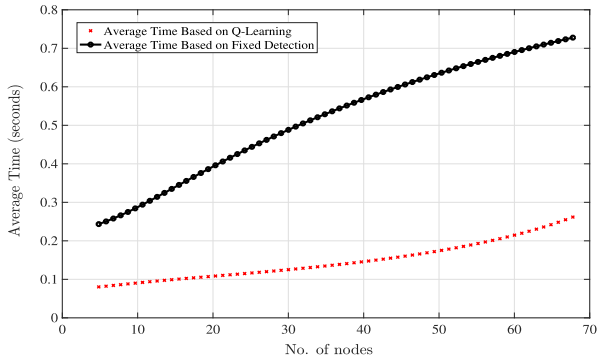


FIGURE 2. Average time for the detection of impersonation attack.

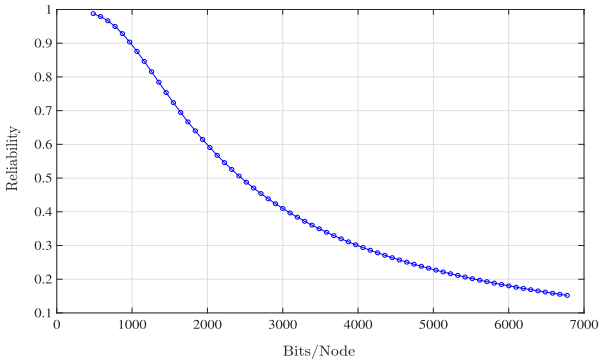


FIGURE 3. Reliability of the receiver to detect bits/node.

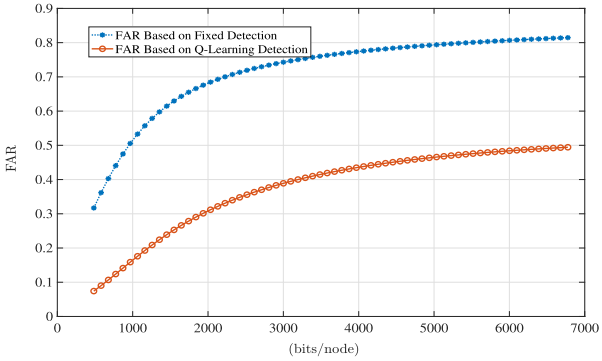


FIGURE 4. Accuracy of FAR at the receiver end.

of the impersonator's channel gain to that of the authentic transmitter. Therefore, we calculate the FAR and MDR based on fixed detection and Q-learning. The values of k, b, and ρ are taken as 3 dB, 0.2, and 10 dB, respectively. The reason behind these two experiments is that by increasing the number of nodes, the FAR and MDR will increase. Because it will be difficult for the receiver to detect the impersonated packet and an authentic packet as the number of nodes increases.

However, we compare FAR and MDR on the basis of fixed detection and Q-learning. From Fig. 4, we can clearly notice that the probability of FAR in Q-learning is lower than the fixed detection. Hence, it is concluded that the receiver notice the packet more accurately than the fixed detection rate.

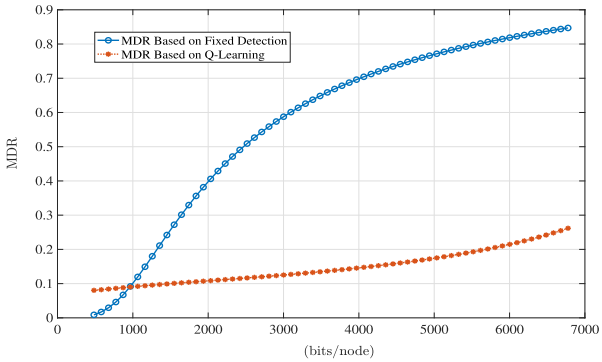


FIGURE 5. Accuracy of MDR at the receiver end.

On the basis of Q-learning, there is less chance that a legitimate node sends an authentic packet, but the receiver notices it as non-legitimate packet. Similarly, in the case of MDR, the Q-learning based authentication outperform than the fixed detection rate as shown in Fig. 5. In result, the accuracy of receiver to detect the legitimate and non-legitimate packet based on Q-learning is outperform than the fixed detection rate. Consequently, we also calculate the AER in our next experiment to find out the performance of Q-learning and fixed detection rate. We calculate the AER for the fixed and Q-learning threshold value on the basis of FAR and MDR, as depict in Fig. 6. It is clear from Fig. 6 that the AER for the fixed value of threshold is higher than the Q-learning. Hence, the accuracy of receiver based on Q-learning to detect the impersonation attack is better than the fixed detection rate.

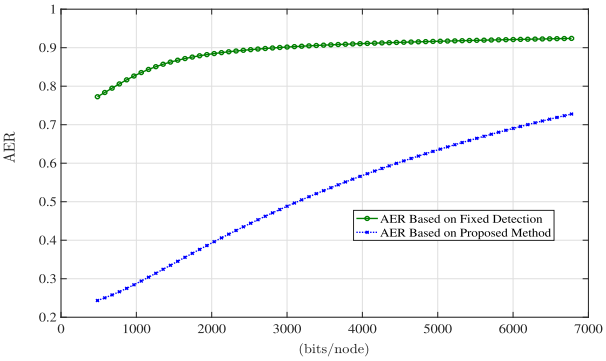


FIGURE 6. AER for fixed and Q-learning based on FAR and MDR.

IV. DISCUSSION

Reinforcement learning (RL) is a subset of machine learning algorithms that learns by exploring its environment. Unlike supervised learning, which trains on labeled datasets, RL achieves its stated objective by receiving positive or negative rewards for the actions that it takes. The environments in which RL works can be both simulated and real-world environments, although real-world environments are seldom used for training RL algorithms. Therefore, in our work, the rewards are based on the detection of authentic and

non-authentic packets and the actions are taken by the receiver correspondingly. This is justified from the simulation results. However, using RL, is that one does not really know what should be the correct answer is, or does not have the labeled data at hand, with the algorithm exploring its state space and achieving the given objective. Therefore, we tried to figure out the how the receiver can detect the impersonation attack through Q-learning. Comparatively, the results based on Q-learning are better than the fixed detection.

From the simulation results, it is concluded that reinforcement learning technique outperformed than the fixed detection values. From Fig. 4, it is reported that the probability of FAR based on Q-learning is approximately 30 % better than the fixed detection. It means that the receiver can automatically learn the environment from the CSI and easily distinguish between the authentic and non-authentic packets. Similarly, the probability of MDR is approximately 60 % better than the fixed detection. Moreover, the MDR at receiver through Q-learning does not increase and remain in the steady state. On the side, the probability of MDR at fixed detection rapidly increases. This is because the receiver does not recognize the authentic and un-authentic users, and hence they are also considered the non-authentic packet as an authentic one in the fixed detection. Finally, the AER is also measured in our results to find out the average error probability between Q-learning and fixed detection. However, this experiment is based on the probability of FAR and MDR. It seems that the AER is increased rapidly based on Q-learning but still it is lower than the fixed detection rate, and is almost 20 % to 60 % lower than the fixed detection.

V. CONCLUSION

In this work, we investigate the PLS that exploits the radio channel information between end user and fog node to detect the impersonation attack in fog computing network. We find out the exact channel parameters between end user and fog node. The work is formulated as zero sum game for fixed detection. The PLS authentication Q-learning scheme is proposed for a dynamic environment. Our proposed scheme shows that the impersonation detection is robust against dynamic environment. The simulation results show that the proposed impersonation detection scheme outperforms fixed detection based on zero sum game. For instance, it is concluded that as the number of nodes increases, the accuracy of receiver (FAR and MDR) on the basis of Q-learning to detect the legitimate and non-legitimate is higher than the fixed detection. Similarly, in the case of AER, the accuracy of receiver based on Q-learning to detect the impersonation attack is approximately 20 % to 60 % better than the fixed detection rate. Since the impersonation detection with Q-learning intensifies the learning speed over the fixed detection, the implementation of authentication is efficiently improved. In our future work, we will tackle diverse security threats for channel authentication, device authentication, spoofing attack, jamming and anti jamming, confidentiality, and denial of service (DoS) attacks through reinforcement learning technique.

REFERENCES

[1] "Cisco visual networking index: Global mobile data traffic forecast update, 2013–2018," Cisco, San Jose, CA, USA, White Paper, 2017.

[2] 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.

[3] Z. Ma *et al.*, "The role of data analysis in the development of intelligent energy networks," *IEEE Netw.*, vol. 31, no. 5, pp. 88–95, Sep. 2017.

[4] M. Waqas, M. Zeng, Y. Li, D. Jin, and Z. Han, "Mobility assisted content transmission for device-to-device communication underlaying cellular networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6410–6423, Jul. 2018.

[5] A. M. Rahmani *et al.*, "Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Gener. Comput. Syst.*, vol. 78, pp. 641–658, Jan. 2018.

[6] Z. Ma, H. Yu, W. Chen, and J. Guo, "Short utterance based speech language identification in intelligent vehicles with time-scale modifications and deep bottleneck features," *IEEE Trans. Veh. Technol.*, to be published.

[7] M. Zeng, Y. Li, K. Zhang, M. Waqas, and D. jin, "Incentive mechanism design for computation offloading in heterogeneous fog computing: A contract-based approach," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 1–6.

[8] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1826–1857, 3rd Quart., 2018.

[9] L. F. Bittencourt, J. Diaz-Montes, R. Buyya, O. F. Rana, and M. Parashar, "Mobility-aware application scheduling in fog computing," *IEEE Cloud Comput.*, vol. 4, no. 2, pp. 26–35, Mar./Apr. 2017.

[10] J. Li, J. Jin, D. Yuan, and H. Zhang, "Virtual fog: A virtualization enabled fog computing framework for Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 121–131, Feb. 2018.

[11] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1054–1079, 2nd Quart., 2017.

[12] A. Diro and N. Chilamkurti, "Leveraging LSTM networks for attack detection in fog-to-things communications," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 124–130, Sep. 2018.

[13] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 44–58, Jan. 2013.

[14] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

[15] M. Waqas, M. Ahmed, Y. Li, D. Jin, and S. Chen, "Social-aware secret key generation for secure device-to-device communication via trusted and non-trusted relays," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3918–3930, Jun. 2018.

[16] M. Mukherjee *et al.*, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.

[17] Z. Ma, J.-H. Xue, A. Leijon, Z.-H. Tan, Z. Yang, and J. Guo, "Decorrelation of neutral vector variables: Theory and applications," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 1, pp. 129–143, Jan. 2018.

[18] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 644–657, Mar. 2018.

[19] J. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4519–4528, Oct. 2018.

[20] C. Hu, A. Alhothaily, A. Alrawais, X. Cheng, C. Sturtivant, and H. Liu, "A secure and verifiable outsourcing scheme for matrix inverse computation," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Atlanta, GA, USA, Oct. 2017, pp. 1–9.

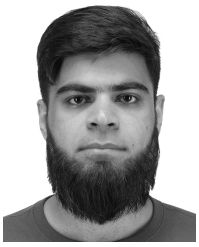
[21] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An attribute-based encryption scheme to secure fog communications," *IEEE Access*, vol. 5, pp. 9131–9138, 2017.

[22] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in Internet of Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1143–1155, Oct. 2017.
[23] J. R. Riehl and M. Cao, "A centrality-based security game for multi-hop networks," *IEEE Trans. Control Netw. Syst.*, to be published.
[24] Z. Ma, Y. Lai, W. B. Kleijn, Y. Song, L. Wang, and J. Guo, "Variational Bayesian learning for Dirichlet process mixture of inverted Dirichlet distributions in non-Gaussian image feature modeling," *IEEE Trans. Neural Netw. Learn. Syst.*, to be published.
[25] Z. Ma and A. Leijon, "Bayesian estimation of beta mixture models with variational inference," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 11, pp. 2160–2173, Nov. 2011.
[26] Z. Ma, A. E. Teschendorff, A. Leijon, Y. Qiao, H. Zhang, and J. Guo, "Variational Bayesian matrix factorization for bounded support data," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 37, no. 4, pp. 876–889, Apr. 2015.
[27] L. Xiao, Y. Li, G. Han, H. Dai, and H. V. Poor, "A secure mobile crowdsensing game with deep reinforcement learning," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 35–47, Jan. 2018.
[28] L. Xiao, D. Jiang, D. Xu, H. Zhu, Y. Zhang, and V. Poor, "Two-dimensional antijamming mobile communication based on reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9499–9512, Oct. 2018.
[29] 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.

SHANSHAN TU received the Ph.D. degree from the Computer Science Department, Beijing University of Posts and Telecommunications, in 2014. From 2013 to 2014, he visited the University of Essex for national joint doctoral training. He was with the Department of Electronic Engineering, Tsinghua University, as a Post-Doctoral Researcher, from 2014 to 2016. He is currently an Assistant Professor with the Faculty of Information Technology, Beijing University of Technology, China. His research interests are in the areas of cloud computing, MEC, and information security techniques.

MUHAMMAD WAQAS received the B.Sc. and M.Sc. degrees from the Department of Electrical Engineering, University of Engineering and Technology at Peshawar, Peshawar, Pakistan, in 2009 and 2014, respectively. From 2012 to 2015, he was with the Sarhad University of Science and Information Technology, Peshawar, as an Assistant Professor and a Program Coordinator.

He is currently pursuing the Ph.D. degree with the Beijing National Research Center for Information Science and Technology, Department of Electronic Engineering, Tsinghua University, Beijing, China. He has several research publications in the IEEE journals and conferences. His current research interests are in the areas of networking and communications, including 5G networks, D2D communication resource allocation and physical layer security and information security, mobility investigation in D2D communication, fog computing, and MEC.



SADAQAT UR REHMAN received the B.Sc. degree from the Department of Computer Systems Engineering, University of Engineering and Technology at Peshawar, Peshawar, in 2011, and the M.Sc. degree from the Department of Electrical Engineering, Sarhad University of Science and Information Technology, Peshawar, Pakistan, in 2014. He served as a Lecturer with the Sarhad University of Science and Information Technology from 2012 to 2015.

He is currently pursuing the Ph.D. degree with the Tsinghua National Laboratory for Information Science and Technology, Department of Electronic Engineering, Tsinghua University, Beijing, China. He has a range of publications in the conferences and journals of repute in his research fields. His current research interests are in the areas of deep learning, including multimedia information retrieval, convolution neural networks, unsupervised learning algorithms, and optimization techniques.

MUHAMMAD AAMIR received the B.Sc. degree from the University of Engineering and Technology at Peshawar, Peshawar, Pakistan, in 2006, and the M.Sc. degree (Hons.) from the CECOS University of Information Technology and Emerging Sciences, Peshawar. He is currently an Associate Professor with the Faculty of Engineering, CECOS University of Information Technology and Emerging Sciences, from 2011 to 2018.

He is currently pursuing the Ph.D. degree with the School of Engineering, Edith Cowan University, Joondalup, Australia. He has different research publications in international Journals. His current research interest includes machining, materials, intelligent algorithms, and optimization techniques. He received the Best Faculty Member Award in 2012 from CECOS University and the Fazaia Educational Welfare Scheme Excellence Award in 2017. He also received the Higher Degree Research Scholarship from Edith Cowan University.

OBAID UR REHMAN received the B.Sc. degree from the University of Engineering and Technology at Peshawar, Peshawar, Pakistan, the M.Sc. degree in computer engineering from the University of Liverpool, Liverpool, U.K., and the Ph.D. degree in electrical engineering from Zhejiang University, China. He is currently an Assistant Professor with the Department of Electrical Engineering, Sarhad University of Science and Information Technology. His research interests are optimization techniques, genetic algorithms, and computational electromagnetics. He has a range of publications in reputed conferences and journals in his research fields.

JIANBIAO ZHANG received the B.S., M.S., and Ph.D. degrees from Northwestern Polytechnic University, Xi'an, Shaanxi, China, in 1992, 1995, and 1999, respectively. From 1999 to 2001, he was a Post-Doctoral Fellow with Beihang University, China. He is currently a Professor and a Ph.D. supervisor with the College of Computer Science and Technology, Beijing University of Technology. His research interests include network and information security, and trusted computing.

CHIN-CHEN CHANG (F'98) received the B.Sc. degree in applied mathematics and the M.Sc. degree in computer and decision sciences from National Tsing Hua University, Hsinchu, Taiwan, and the Ph.D. degree in computer engineering from National Chiao Tung University, Hsinchu. He was with National Chung Cheng University, Chiayi, Taiwan, from 1989 to 2005. He was an Associate Professor with National Chiao Tung University, a Professor with National Chung Hsing University, Taichung, Taiwan, and a Chair Professor with National Chung Cheng University.

He was invited to serve as a visiting professor, a chair professor, an honorary professor, an honorary director, an honorary chairman, a distinguished alumnus , a distinguished researcher, and a research fellow with universities and research institutes. He was a Visiting Researcher and a Visiting Scientist with Tokyo University, Tokyo, Japan, and Kyoto University, Kyoto, Japan, respectively. He also served as the Chairman of the Institute of Computer Science and Information Engineering, the Dean of the College of Engineering, a Provost, the Acting President of National Chung Cheng University, and the Director of the Advisory Office, Ministry of Education, Taipei, Taiwan. He has been a Chair Professor with the Department of Information Engineering and Computer Science, Feng Chia University, Taichung, since 2005. His current research interests include database design, computer cryptography, image compression, and data structures. He is currently a fellow of the IEE, U.K. He was a recipient of several research awards and honorary positions by and in prestigious organizations both nationally and internationally.