Liang Xiao, Xiaoyue Wan, Xiaozhen Lu,
Yanyong Zhang, and Di Wu

IoT Security Techniques Based on Machine Learning

How do IoT devices use AI to enhance security?

INTERNET OF THINGS—ISTOCKPHOTO.COM/IAREMENKO
CIRCUITS—IMAGE LICENSED BY INGRAM PUBLISHING

Digital Object Identifier 10.1109/MSP.2018.2825478
Date of publication: 28 August 2018

The Internet of things (IoT), which integrates a variety of devices into networks to provide advanced and intelligent services, has to protect user privacy and address attacks such as spoofing attacks, denial of service (DoS) attacks, jamming, and eavesdropping. We investigate the attack model for IoT systems and review the IoT security solutions based on machine-learning (ML) techniques including supervised learning, unsupervised learning, and reinforcement learning (RL). ML-based IoT authentication, access control, secure offloading, and malware detection schemes to protect data privacy are the focus of this article. We also discuss the challenges that need to be addressed to implement these ML-based security schemes in practical IoT systems.

Introduction

The IoT facilitates integration between the physical world and computer communication networks, and applications (apps) such as infrastructure management and environmental monitoring make privacy and security techniques critical for future IoT systems [1]–[3]. Consisting of radio-frequency identifications (RFIDs), wireless sensor networks (WSNs), and cloud computing [4], IoT systems have to protect data privacy and address security issues such as spoofing attacks, intrusions, DoS attacks, distributed DoS (DDoS) attacks, jamming, eavesdropping, and malware [5], [6]. For instance, wearable devices that collect and send the user health data to a connected smartphone have to avoid privacy information leakage.

It's generally prohibitive for IoT devices with restricted computation, memory, radio bandwidth, and battery resources to execute computational-intensive and latency-sensitive security tasks, especially under heavy data streams [7]. However, most existing security solutions generate a heavy computation and communication load for IoT devices, and outdoor IoT devices such as cheap sensors with lightweight security protections are usually more vulnerable to attacks than computer systems. As shown in Figure 1, we investigate IoT authentication, access control, secure offloading, and malware detection.

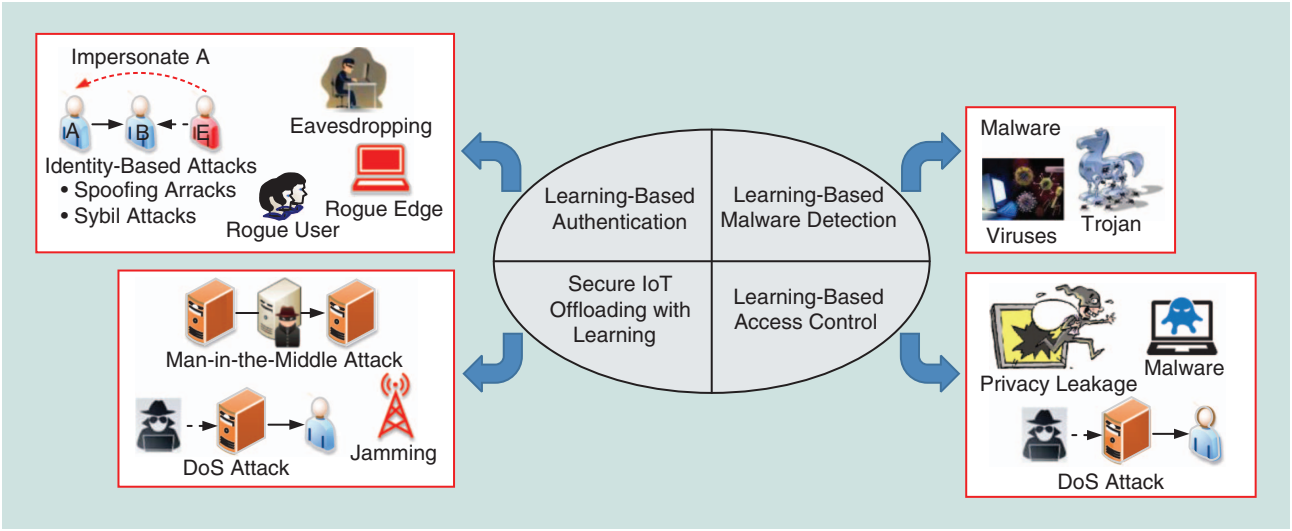

FIGURE 1. An illustration of the threat model in the IoT.

- Authentication helps IoT devices distinguish the source nodes and address identity-based attacks such as spoofing and Sybil attacks [8].
- Access control prevents unauthorized users from accessing the IoT resources [9].
- Secure offloading techniques enable IoT devices to use the computation and storage resources of the servers and edge devices for computational-intensive and latency-sensitive tasks [10].
- Malware detection protects IoT devices from privacy leakage, power depletion, and network performance degradation against malware such as viruses, worms, and Trojans [11].

With the development of ML and smart attacks, IoT devices have to choose a defensive policy and determine the key parameters in the security protocols for the tradeoff in the heterogenous and dynamic networks. This task is challenging as an IoT device with restricted resources usually has difficulty accurately estimating the current network and attack state in time. For example, the authentication performance of the scheme in [8] is sensitive to the test threshold in the hypothesis test, which depends on both the radio propagation model and the spoofing model. Such information is unavailable for most outdoor sensors, leading to a high false alarm or misdetection rate in the spoofing detection.

ML techniques including supervised learning, unsupervised learning, and RL have been widely applied to improve network security as summarized in Table 1, such as authentication, access control, antijamming offloading, and malware detection [8]–[22].

- Supervised learning techniques such as support vector machines (SVMs), naive Bayes, K-nearest neighbor (K-NN), neural networks (NNs), deep NNs (DNNs), and random forest can be used to label the network traffic or app traces of IoT devices to build the classification or regression model [9]. For example, IoT devices can use SVMs to detect network intrusion [9] and spoofing attacks [12], apply K-NNs in network intrusion [13] and malware [14] detection, and utilize NNs to detect network intrusion [15] and DoS attacks [16]. Naive Bayes can be applied by IoT devices in intrusion detection [9], and random forest classifier can be used to detect malware[14]. IoT devices with sufficient computation and memory resources can utilize DNNs to detect spoofing attacks [23].
- Unsupervised learning does not require labeled data in the supervised learning and investigates the similarity between the unlabeled data to cluster them into different groups [9]. For example, IoT devices can use multivariate correlation analysis to detect DoS attacks [17] and apply the infinite Gaussian mixture model (IGMM) in the physical (PHY)-layer authentication with privacy protection [18].
- RL techniques such as Q-learning, Dyna-Q, postdecision state (PDS) [24], and deep Q-network (DQN) [25] enable an IoT device to choose security protocols as well as key parameters against various attacks via trial and error [8]. For example, Q-learning as a model-free RL technique has been used to improve the performance of authentication [8], antijamming offloading [10], [19], [20], and malware detection [11], [21]. IoT devices can apply Dyna-Q in authentication and malware detection [11], use PDS to detect malware [11], and DQN in antijamming transmissions [22].

IoT attack model

Consisting of things, services, and networks, IoT systems are vulnerable to network, physical, and software attacks as well as privacy leakage. As shown in Figure 1, we focus on the IoT security threats as follows:

- *DoS attackers*: The attackers flood the target server with superfluous requests to prevent IoT devices from obtaining services [4]. One of the most dangerous types of a DoS attack is when DDoS attackers use thousands of Internet protocol addresses to request IoT services, making it difficult for the server to distinguish the legitimate IoT devices from attackers. Distributed IoT devices with lightweight

security protocols are especially vulnerable to DDoS attacks [5].

- *Jamming*: Attackers send fake signals to interrupt the ongoing radio transmissions of IoT devices and further deplete the bandwidth, energy, central processing units (CPUs), and memory resources of IoT devices or sensors during their failed communication attempts [22].
- *Spoofing*: A spoofing node impersonates a legal IoT device with its identity such as the medium access control (MAC) address and RFID tag to gain illegal access to the IoT system and can further launch attacks such as DoS and man-in-the-middle attacks [8].
- *Man-in-the-middle attack*: A man-in-the-middle attacker sends jamming and spoofing signals with the goal of secretly monitoring, eavesdropping, and altering the private communication between IoT devices [4].
- *Software attacks*: Mobile malware such as Trojans, worms, and viruses can result in privacy leakage, economic loss, power depletion, and network performance degradation of IoT systems [11].
- *Privacy leakage*: IoT systems have to protect user privacy during data caching and exchange. Some caching owners are curious about the data content stored on their devices and analyze and sell such IoT privacy information. Wearable devices that collect user's personal information such as location and health information have witnessed an increased risk of personal privacy leakage [26].

Learning-based authentication

Traditional authentication schemes are not always applicable to IoT devices with limited computation, battery, and memory resources to detect identity-based attacks such as spoofing and Sybil attacks. PHY-layer authentication techniques that exploit the spatial decorrelation of the PHY-layer features of radio channels and transmitters such as the received signal strength indicators (RSSIs), received signal strength (RSS), channel impulse responses (CIRs) of the radio channels, channel state information (CSI), and the MAC address can provide lightweight security protection for IoT devices without leaking user privacy information [8].

PHY-layer authentication methods such as [8] build hypothesis tests to compare the PHY-layer feature of the message under test with the record of the claimed transmitter. Their authentication accuracy depends on the test threshold in the hypothesis test. However, it is challenging for an IoT device to choose an appropriate test threshold of the authentication due to the radio environment and the unknown spoofing model. The IoT device estimates the false alarm and misdetection rate of the spoofing detection at the last time slot, and the state of the learning consists of the false alarm and misdetection rate. The future state observed by the IoT device is independent of the previous states and actions if the current state and test threshold are known. Therefore, the test threshold selection in the IoT authentication in the repeated game against spoofing attacks can be viewed as a Markov decision process (MDP) with finite states.

The Q-learning-based authentication as proposed in [8] depends on the RSSI of the signals under test and enables an IoT device to achieve the optimal test threshold and improve the utility and the authentication accuracy. For example, the Q-learning-based authentication reduces the average authentication error rate by 64.3%, to less than 5%, and increases the utility by 14.7% compared with the PHY-authentication with a fixed threshold in an experiment performed in a $12 \times 9.5 \times 3$ m^3 lab with 12 transmitters [8].

Supervised learning techniques such as distributed Frank-Wolfe (dFW) and incremental aggregated gradient (IAG) can also be applied in IoT systems to improve spoofing resistance.

Table 1. ML-based IoT security methods.

Attacks	Security Techniques	ML Techniques	Performance
DoS	Secure IoT offloading	NN [16]	Detection accuracy
	Access control	Multivariate correlation analysis [17]	Root mean error
		Q-learning [21]	
Jamming	Secure IoT offloading	Q-learning [19], [20]	Energy consumption SINR
		DQN [22]	
Spoofing	Authentication	Q-learning [8]	Average error rate
		Dyna-Q [8]	Detection accuracy
		SVM [12]	Classification accuracy
		DNN [23]	False alarm rate
		dFW [27]	Missdetection rate
		Incremental aggregated gradient [27]	
Intrusion	Access control	SVM [9]	Classification accuracy
		Naive Bayes [9]	False alarm rate
		K-NNs [13]	Detection rate
		NN [15]	Root mean error
Malware	Malware detection Access control	Q/Dyna-Q/PDS [11]	Classification accuracy
		Random forest [14]	False positive rate
		K-NNs [14]	True positive rate
			Detection accuracy
			Detection latency
Eavesdropping	Authentication	Q-learning [10]	Proximity passing rate
		Nonparametric Bayesian [18]	Secrecy data rate

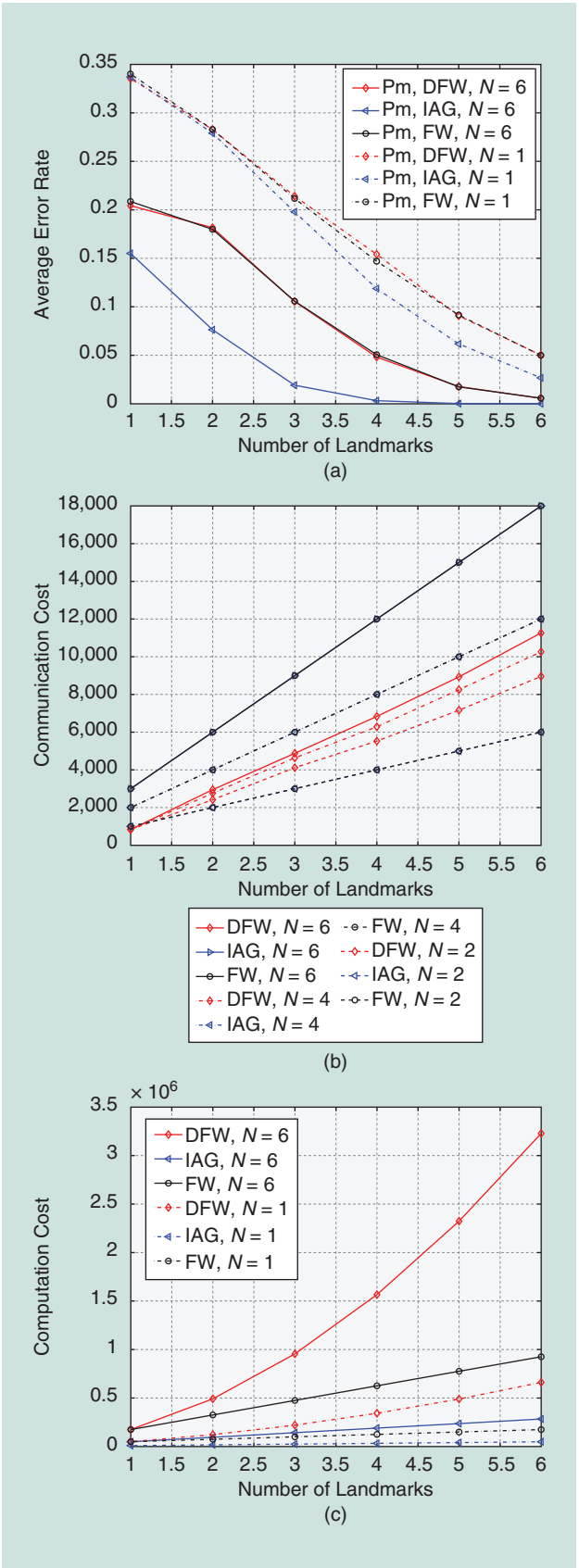

FIGURE 2. The performance of a PHY-layer authentication system with a different number of antennas at each landmark [27]: (a) average error rate, (b) communication cost, and (c) computation cost.

The authentication scheme in [27] exploits the RSSIs received by multiple landmarks and uses logistic regression to avoid being restricted to a known radio channel model. By applying the dFW and IAG algorithms to estimate the parameters of the logistic regression model, this authentication scheme saves communication overhead and improves spoofing detection accuracy. As shown in Figure 2, the average error rates of the dFW-based authentication and the IAG-based scheme are 6% and less than 10^{-4}, respectively, in the simulation with six landmarks, each equipped with six antennas. The dFW-based authentication reduces the communication overhead by 37.4%, while the IAG reduces the computation overhead by 71.3% compared with the Frank-Wolfe-based scheme in this case [27].

Unsupervised learning techniques such as IGMM can be applied in proximity-based authentication to authenticate the IoT devices in the proximity without leaking the localization information of the devices. For instance, the authentication scheme as proposed in [18] uses IGMM, a nonparametric Bayesian method to avoid the "overfitting" problem and, thus, adjust the model complexity, to evaluate the RSSIs and the packet arrival time intervals of the ambient radio signals to detect spoofers outside the proximity range. This scheme reduces the detection error rate by 20% to 5%, compared with the Euclidean distance-based authentication [18] in the spoofing detection experiments in an indoor environment.

As shown in Figure 3, this scheme requests the IoT device under test to send the ambient signals' features such as the RSSIs, MAC addresses, and packet arrival time interval of the ambient signals received during a specific time duration. The IoT device extracts and sends the ambient signals' features to the legal receiver. Upon receiving such authentication messages, the receiver applies IGMM to compare the reported signal features with those of the ambient signals observed in the proximity-based test. The receiver provides the IoT device passing the authentication with access to the IoT resources.

Finally, deep-learning techniques such as DNNs can be applied for IoT devices with sufficient computation and memory resources to further improve the authentication accuracy. The DNN-based user authentication as presented in [23] extracts the CSI features of the Wi-Fi signals and applies DNNs to detect spoofing attackers. The spoofing detection accuracy of this scheme is about 95%, and the user identification accuracy is 92.34% [23].

Learning-based access control

It is challenging to design access control for IoT systems in heterogeneous networks with multiple types of nodes and multisource data [9]. ML techniques such as SVMs, K-NNs, and NNs have been used for intrusion detection [15]. For instance, the DoS attack detection as proposed in [17] uses multivariate correlation analysis to extract the geometrical correlations between network traffic features. This scheme increases the detection accuracy by 3.05% to 95.2% compared with the triangle-area-based nearest-neighbors approach using the KDD Cup 99 data set [17].

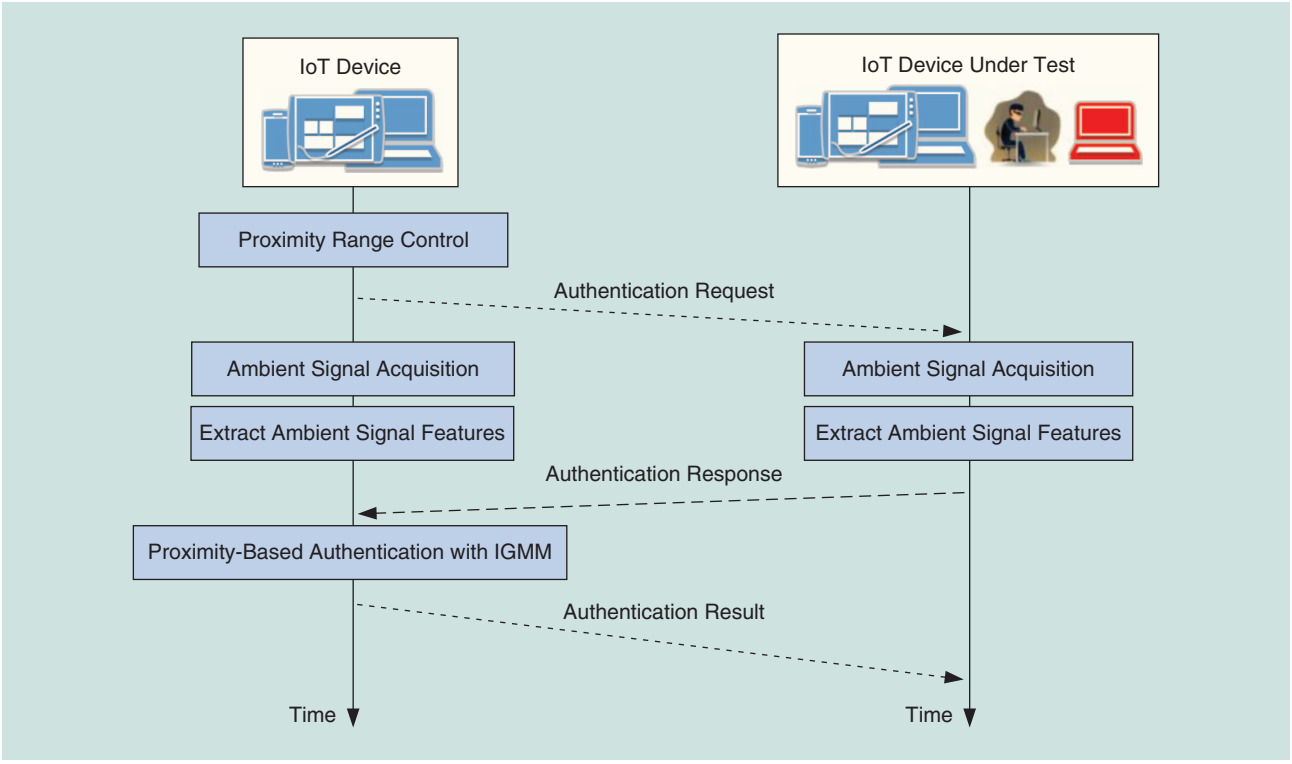

FIGURE 3. An illustration of ML-based authentication in IoT systems.

IoT devices such as outdoor sensors usually have strict resource and computation constraints, yielding challenges for anomaly intrusion detection techniques and thus degrading the intrusion detection performance for IoT systems. ML techniques help build lightweight access control protocols to save energy and extend the lifetime of IoT systems. For example, the outlier detection scheme as developed in [13] applies K-NNs to address the problem of unsupervised outlier detection in WSNs and offers flexibility to define outliers with reduced energy consumption. This scheme can save the maximum energy by 61.4% compared with the centralized scheme with similar average energy consumption [13].

The multilayer perceptron (MLP)-based access control as presented in [16] utilizes the NN with two neurons in the hidden layer to train the connection weights of the MLP and compute the suspicion factor that indicates whether an IoT device is the victim of DoS attacks. This scheme utilizes backpropagation (BP) that applies the forward computation and error BP and particle swarm optimization (PSO) as an evolutionary computation technique that utilizes particles with adjustable velocities to update the connection weights of the MLP. The IoT device under test shuts down the MAC- and PHY-layer functions to save energy and extend the network life if the output of the MLP exceeds a threshold.

Supervised learning techniques such as SVMs are used to detect multiple types of attacks for Internet traffic [28] and the smart grid [12]. For instance, a lightweight attack-detection mechanism as proposed in [28] uses an SVM-based hierarchical structure to detect traffic flooding attacks. In the attack experiment, the data set collector system gathered Simple Network Management Protocol (SNMP) management information base data from the victim system using SNMP query messages. Experiment results show that this scheme can achieve an attack detection rate over 99.40% and classification accuracy over 99.53% [28].

Secure IoT offloading with learning

IoT offloading has to address the attacks launched from the PHY- or MAC- layer attacks, such as jamming, rogue edge devices, rogue IoT devices, eavesdropping, man-in-the-middle attacks, and smart attacks [29]. As the future state observed by an IoT device is independent of the previous states and actions for a given state and offloading strategy in the current time slot, the mobile offloading strategy chosen by the IoT device in the repeated game with jammers and interference sources can be viewed as an MDP with finite states [10]. RL techniques can be used to optimize the offloading policy in dynamic radio environments.

Q-learning, as a model-free RL technique, is convenient to implement with low computation complexity. For example, IoT devices can utilize the Q-learning-based offloading as proposed in [10] to choose their offloading data rates against jamming and spoofing attacks. As illustrated in Figure 4, the IoT device observes the task importance, the received jamming power, the radio channel bandwidth, and the channel gain to formulate its current state, which is the basis to choose the offloading policy according to the Q-function. The Q-function is the expected discounted long-term reward for each action-state pair and

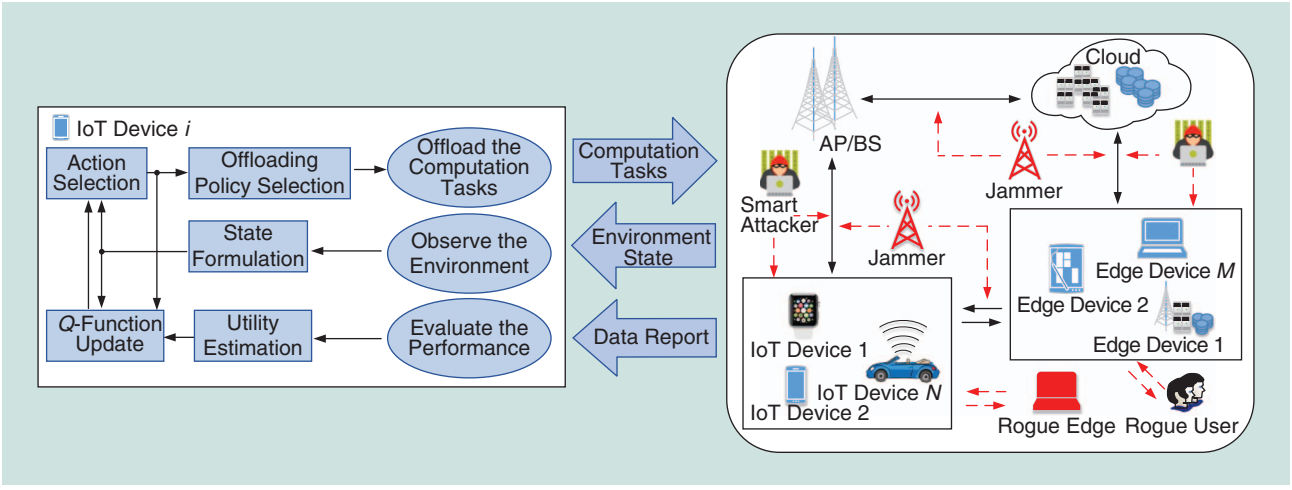

FIGURE 4. An illustration of ML-based offloading. AP: access point; BS: base station.

represents the knowledge obtained from the previous antijamming offloading. The Q-values are updated via the iterative Bellman equation in each time slot according to the current offloading policy, the network state, and the utility received by the IoT device against jamming.

The IoT device evaluates the signal-to-interference-plus-noise ratio (SINR) of the received signals, secrecy capacity, offloading latency, and energy consumption of the offloading process and estimates the utility in this time slot. The IoT device applies the ϵ-greedy algorithm in the offloading policy selection, in which the offloading policy with the max Q-value is selected with a high probability and the other policies are chosen with a small probability. Therefore, the IoT device makes a tradeoff between the exploration (i.e., to avoid being trapped in the local optimal strategy) and the exploitation (i.e., to improve the long-term reward). This scheme reduces the spoofing rate by 50% and decreases the jamming rate by 8% compared with a benchmark strategy as presented in [10].

According to the Q-learning-based antijamming transmission as proposed in [19], an IoT device can apply Q-learning to choose the radio channel to access the cloud or edge device without being aware of the jamming and interference model in IoT systems. As shown in Figure 4, the IoT device observes the center frequency and radio bandwidth of each channel to formulate the state and chooses the optimal offloading channel based on the current state and Q-function. Upon receiving the computation report, the IoT device evaluates the utility and updates the Q values. Simulation results in [19] show that this scheme increases the average cumulative reward by 53.8% compared with the benchmark random channel selection strategy.

Q-learning also helps IoT devices achieve the optimal subband from the radio spectrum band to resist jamming and interference from other radio devices. As shown in Figure 4, the IoT device observes the spectrum occupancy to formulate the state and selects the spectrum band accordingly. In an experiment against a sweeping jammer and in the presence of two wideband autonomous cognitive radios with ten subbands, this scheme increases the jamming cost by 44.3% compared with the benchmark subband selection strategy in [20].

The DQN-based antijamming transmission as developed in [22] accelerates the learning speed for IoT devices with sufficient computation and memory resources to choose the radio frequency channel. This scheme applies the convolutional NN (CNN) to compress the state space for large-scale networks with a large number of IoT devices and jamming policies in a dynamic IoT system and thus increase the SINR of the received signals. More specifically, the CNN consists of two convolutional layers and two fully connected layers. The weights of the CNN are updated based on the stochastic gradient descent algorithm according to the previous experience in the memory pool. The output of the CNN is used for estimating the values of the Q-function for each antijamming transmission policy. This scheme increases the SINR of the received signals by 8.3% and saves 66.7% of the learning time compared with the Q-learning scheme in the offloading against jamming attacks [22].

Learning-based IoT malware detection

IoT devices can apply supervised learning techniques to evaluate the runtime behaviors of the apps in malware detection. In the malware detection scheme as developed in [14], an IoT device uses K-NNs and random forest classifiers to build the malware-detection model. As illustrated in Figure 5, the IoT device filters the TCP packets and selects the features among various network features including the frame number and length, labels them, and stores these features in the database. The K-NN-based malware detection assigns the network traffic to the class with the largest number of objects among its K-NNs. The random forest classifier builds the decision trees with the labeled network traffic to distinguish malware. According to the experiments in [14], the true positive rates of the K-NN-based malware detection and random forest-based scheme with the MalGenome data set are 99.7% and 99.9%, respectively.

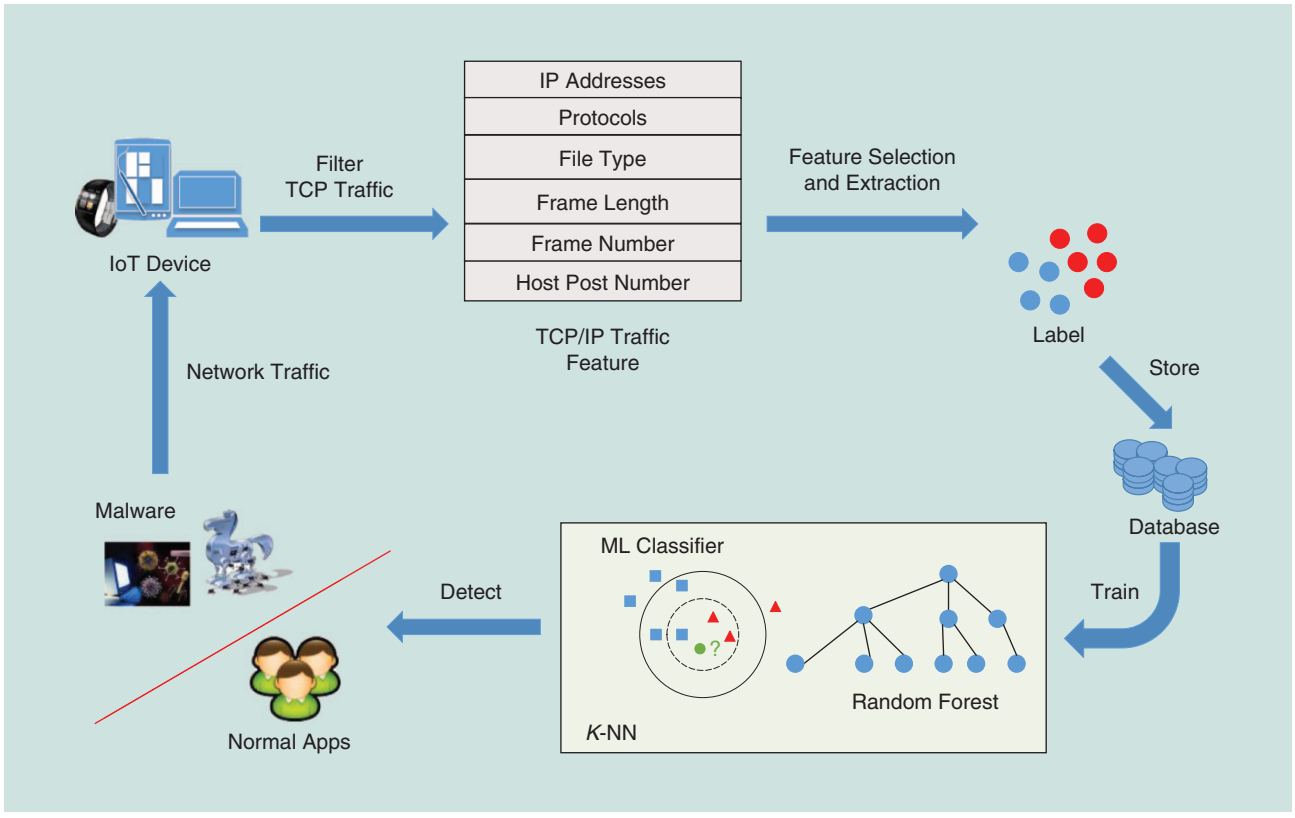

FIGURE 5. An illustration of ML-based malware detection.

IoT devices can offload app traces to the security servers at the cloud or edge devices to detect malware with a larger malware database, faster computation speed, larger memories, and more powerful security services. The optimal proportion of the app traces to offload depends on the radio channel state to each edge device and the number of the generated app traces. RL techniques can be applied for an IoT device to achieve the optimal offloading policy in a dynamic malware-detection game without being aware of the malware and app-generation models [11].

In a malware-detection scheme as developed in [11], an IoT device can apply Q-learning to achieve the optimal offloading rate without knowing the trace generation and radio bandwidth model of the neighboring IoT devices. As shown in Figure 6, the IoT device divides real-time app traces into a number of portions and observes the user density and radio channel bandwidth to formulate the current state. The IoT device estimates the detection accuracy gain, detection latency, and energy consumption to evaluate the utility received in this time slot. This scheme improves the detection accuracy by 40%, reduces the detection latency by 15%, and increases the utility of the mobile devices by 47% compared with the benchmark offloading strategy in [11] in a network consisting of 100 mobile devices.

The Dyna-Q-based malware detection scheme as presented in [11] exploits the Dyna architecture to learn from hypothetical experience and finds the optimal offloading strategy. This scheme utilizes both the real defense and virtual experiences generated by the Dyna architecture to improve the learning performance. For instance, this scheme reduces the detection latency by 30% and increases the accuracy by 18% compared with the detection with Q-learning [11].

To address the false virtual experiences of Dyna-Q, especially at the beginning of the learning process, the PDS-based malware detection scheme as developed in [11] utilizes the known radio channel model to accelerate the learning speed. This scheme applies the known information regarding the network, attack, and channel models to improve the exploration efficiency and utilizes Q-learning to study the remaining unknown state space. This scheme increases the detection accuracy by 25% compared with the Dyna-Q-based scheme in a network consisting of 200 mobile devices [11].

Conclusions and future work

In this article, we have identified IoT attack models and learning-based IoT security techniques, including IoT authentication, access control, malware detection, and secure offloading, which are shown to be promising protection for the IoT. Several challenges have to be addressed to implement the learning-based security techniques in practical IoT systems.

- *Partial state observation*: Existing RL-based security schemes assume that each learning agent knows the accurate state and evaluates the immediate reward for each action in time. In addition, the agent has to tolerate the bad strategies—especially at the beginning of the learning process. However, IoT devices usually have difficulty

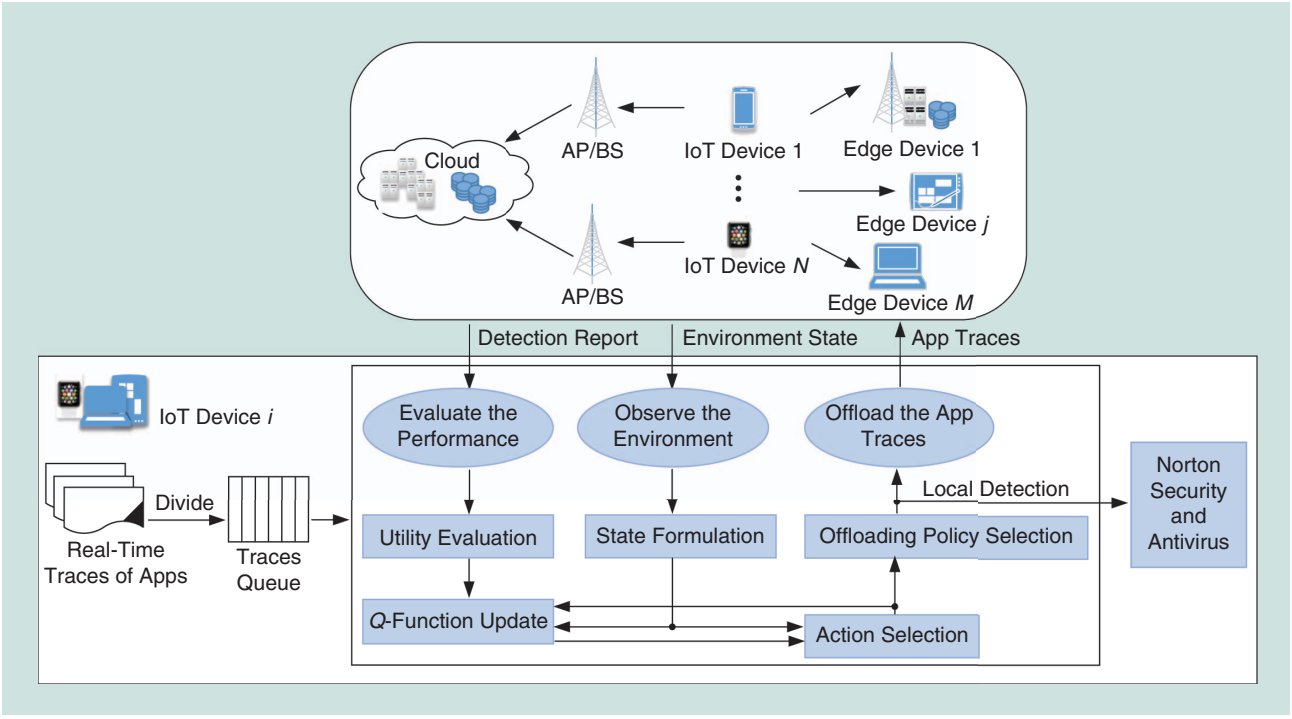

FIGURE 6. An illustration of ML-based malware detection with offloading.

estimating the network and attack state accurately and have to avoid the security disaster due to a bad policy at the beginning of the learning process. A potential solution is transfer learning [30], which explores existing defense experiences with data mining to reduce random exploration, accelerates the learning speed, and decreases the risks of choosing bad defense policies at the beginning of the learning process. In addition, backup security mechanisms have to be provided to protect IoT systems from the exploration stage in the learning process.

- *Computation and communication overhead*: Many existing ML-based security schemes have intensive computation and communication costs and require a large number of training data and a complicated feature-extraction process [9]. Therefore, new ML techniques with low computation and communication overhead such as dFW have to be investigated to enhance security for IoT systems, especially for the scenarios without cloud-based servers and edge computing.
- *Backup security solutions*: To achieve optimal strategy, the RL-based security methods have to explore the "bad" security policy that sometimes can cause network disaster for IoT systems at the beginning learning stage. The intrusion detection schemes based on unsupervised learning techniques sometimes have misdetection rates that are nonnegligible for IoT systems. Supervised and unsupervised learning sometimes fail to detect the attacks due to oversampling, insufficient training data, and bad feature extraction. Therefore, backup security solutions have to be designed and incorporated with the ML-based security schemes to provide reliable and secure IoT services.

Acknowledgment

This work was supported by the National Natural Science Foundation of China under grants 61671396, 61671398, 61472335, and 61572538; the Fundamental Research Funds for the Central Universities under grant 17LGJC23; the open research fund of the National Mobile Communications Research Laboratory, Southeast University (2018D08); the Open Research Project of the State Key Laboratory of Industrial Control Technology, Zhejiang University, China (ICT1800386); and the U.S. National Science Foundation under grants CNS-1404118, CNS-1423020, and CNS-1149611.

Authors

Liang Xiao (lxiao@xmu.edu.cn) received her B.S. degree in communication engineering from Nanjing University of Posts and Telecommunications, China, in 2000, her M.S. degree in electrical engineering from Tsinghua University, China, in 2003, and her Ph.D. degree in electrical engineering from Rutgers University, New Jersey, in 2009. She is currently a professor in the Department of Communication Engineering, Xiamen University, Fujian, China. She has been an associate editor of *IEEE Transactions on Information Forensics and Security* and *IET Communications*. Her research interests include wireless security, smart grids, and wireless communications. She won the Best Paper Award for the 2016 IEEE International Conference on Computer Communications Big Security Workshop. She has been a visiting professor with Princeton University, Virginia Tech, and the University of Maryland, College Park. She is a Senior Member of the IEEE.

Xiaoyue Wan (23320161153393@stu.xmu.edu.cn) received her B.S. degree in communication engineering from Xiamen

University, Fujian, China, in 2016, where she is currently pursuing her M.S. degree in the same field.

Xiaozhen Lu (23320170155538@stu.xmu.edu.cn) received her B.S. degree in communication engineering from Nanjing University of Posts and Telecommunications, China, in 2017. She is currently pursuing her Ph.D. degree with the Department of Communication Engineering, Xiamen University, Fujian, China. She is a Student Member of the IEEE.

Yanyong Zhang (yyzhang@winlab.rutgers.edu) received her B.S. degree in computer science from the University of Science and Technology of China, Hefei, in 1997. She a professor in the Electrical and Computer Engineering Department at Rutgers University, North Brunswick, New Jersey. She is also a member of the Wireless Information Networking Laboratory. From March to July 2009, she was a visiting scientist at Nokia Research Center, Beijing. She is the recipient of a U.S. National Science Foundation CAREER Award. She is currently an associate editor of *IEEE Transactions on Mobile Computing, IEEE Transactions on Services Computing, ACM/IEEE Transactions on Networking*, and *Elsevier Smart Health*. She has served on technical program committees of many conferences, including the IEEE International Conference on Computer Communications and the International Conference on Distributed Computing Systems. She is a Fellow of the IEEE.

Di Wu (wudi27@mail.sysu.edu.cn) received his B.S. degree from the University of Science and Technology of China, Hefei, in 2000, his M.S. degree from the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, in 2003, and his Ph.D. degree in computer science and engineering from the Chinese University of Hong Kong in 2007. He was a postdoctoral researcher with the Department of Computer Science and Engineering, Polytechnic Institute of New York University, Brooklyn, from 2007 to 2009, advised by Prof. K.W. Ross. He is currently a professor and the assistant dean of the School of Data and Computer Science with Sun Yat-sen University, Guangzhou, China. He was the recipient of the IEEE International Conference on Computer Communications 2009 Best Paper Award. His research interests include cloud computing, multimedia communication, Internet measurement, and network security.

References

[1] X. Li, R. Lu, X. Liang, and X. Shen, "Smart community: An Internet of things application," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 68–75, Nov. 2011.

[2] B. Firner, R. S. Moore, R. Howard, R. P. Martin, and Y. Zhang, "Poster: Smart buildings, sensor networks, and the Internet of things," in *Proc. ACM Conf. Embedded Networked Sensor Systems*, Nov. 2011, pp. 337–338.

[3] Z. Sheng, S. Yang, Y. Yu, and A. Vasilakos, "A survey on the IETF protocol suite for the Internet of things: Standards, challenges, and opportunities," *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 91–98, Dec. 2013.

[4] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *Proc. IEEE Symp. Computers and Communication*, Larnaca, Cyprus, Feb. 2015, pp. 180–187.

[5] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, July 2013.

[6] S. Chen, H. Xu, D. Liu, and B. Hu, "A vision of IoT: Applications, challenges, and opportunities with china perspective," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 349–359, July 2014.

[7] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[8] 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.

[9] M. Abu Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Commun. Surveys Tutorials*, vol. 16, no. 4, pp. 1996–2018, Apr. 2014.

[10] L. Xiao, C. Xie, T. Chen, and H. Dai, "A mobile offloading game against smart attacks," *IEEE Access*, vol. 4, pp. 2281–2291, May 2016.

[11] L. Xiao, Y. Li, X. Huang, and X. J. Du, "Cloud-based malware detection game for mobile devices with offloading," *IEEE Trans. Mobile Comput.*, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.

[12] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Networks and Learning Syst.*, vol. 27, no. 8, pp. 1773–1786, Mar. 2015.

[13] J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," *Knowl. Inform. Syst.*, vol. 34, no. 1, pp. 23–54, Jan. 2013.

[14] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," *Soft Comput.*, vol. 20, no. 1, pp. 343–357, Jan. 2016.

[15] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tutorials*, vol. 18, no. 2, pp. 1153–1176, Oct. 2015.

[16] R. V. Kulkarni and G. K. Venayagamoorthy, "Neural network based secure media access control protocol for wireless sensor networks," in *Proc. Int. Joint Conf. Neural Networks*, Atlanta, GA, June 2009, pp. 3437–3444.

[17] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for Denial-of-Service attack detection based on multivariate correlation analysis," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 447–456, May 2013.

[18] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-based security techniques for mobile users in wireless networks," *IEEE Trans. Inform. Forensics Security*, vol. 8, no. 12, pp. 2089–2100, Oct. 2013.

[19] Y. Gwon, S. Dastangoo, C. Fossa, and H. Kung, "Competing mobile network game: Embracing anti-jamming and jamming strategies with reinforcement learning," in *Proc. IEEE Conf. Communication and Network Security*, National Harbor, MD, Oct. 2013, pp. 28–36.

[20] M. A. Aref, S. K. Jayaweera, and S. Machuzak, "Multi-agent reinforcement learning based cognitive anti-jamming," in *Proc. IEEE Wireless Communication and Networking Conf.*, San Francisco, CA, Mar. 2017, pp. 1–6.

[21] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "SINR-based DoS attack on remote state estimation: A game-theoretic approach," *IEEE Trans. Contr. Network Syst.*, vol. 4, no. 3, pp. 632–642, Apr. 2016.

[22] G. Han, L. Xiao, and H. V. Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," in *Proc. IEEE Int. Conf. Acoustics Speech and Signal Processing*, New Orleans, LA, Mar. 2017, pp. 2087–2091.

[23] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in *Proc. ACM Int Symp. Mobile AdHoc Networking and Computing*, Chennai, India, July 2017, pp. 1–10.

[24] X. He, H. Dai, and P. Ning, "Improving learning and adaptation in security games by exploiting information asymmetry," in *Proc. IEEE Conf. Computer Communication*, Hongkong, China, May 2015, pp. 1787–1795.

[25] V. Mnih, K. Kavukcuoglu, D. Silver, et al., "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, Jan. 2015.

[26] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of things," *J. Netw. Comput. Appl.*, vol. 42, no. 3, pp. 120–134, June 2014.

[27] 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.

[28] J. Yu, H. Lee, M. S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," *Comput.Commun.*, vol. 31, no. 17, pp. 4212–4219, Oct. 2008.

[29] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, no. 3, pp. 680–698, Jan. 2018.

[30] S. J. Pan and Q. Yang, "A survey on transfer learning," *IEEE Trans. Knowledge Data Eng.*, vol. 22, no. 10, pp. 1345–1359, Oct. 2010.

SP