Artificial Intelligence Review (2022) 55:5215–5261
https://doi.org/10.1007/s10462-022-10143-2

The role of artificial intelligence and machine learning in wireless networks security: principle, practice and challenges

Muhammad Waqas[1,2,3] · Shanshan Tu[1] · Zahid Halim[3] · Sadaqat Ur Rehman[4] · Ghulam Abbas[3] · Ziaul Haq Abbas[5]

Published online: 4 February 2022

Abstract
Security is one of the biggest challenges concerning networks and communications. The problem becomes aggravated with the proliferation of wireless devices. Artificial Intelligence (AI) has emerged as a promising solution and a volume of literature exists on the methodological studies of AI to resolve the security challenge. In this survey, we present a taxonomy of security threats and review distinct aspects and the potential of AI to resolve the challenge. To the best of our knowledge, this is the first comprehensive survey to review the AI solutions for all possible security types and threats. We also present the lessons learned from the existing AI techniques and contributions of up-to-date literature, future directions of AI in security, open issues that need to be investigated further through AI, and discuss how AI can be more effectively used to overcome the upcoming advanced security threats.

Keywords Artificial intelligent · Security · Wireless communication · Network security

✉ Muhammad Waqas
engr.waqas2079@gmail.com

Shanshan Tu
sstu@bjut.edu.cn

[1] Research Center of Intelligent Perception and Autonomous Control, Faculty of Information Technology, Beijing University of Technology, Beijing 100124, People's Republic of China

[2] School of Engineering, Edith Cowan University, Perth, WA 6027, Australia

[3] Faculty of Computer Science and Engineering, Ghulam Ishaq Khan (GIK) Institute of Engineering Sciences Technology, Topi 23460, Pakistan

[4] Department of Computer Science, Namal Institute, Mianwali, Pakistan

[5] Faculty of Electrical Engineering, Ghulam Ishaq Khan (GIK) Institute of Engineering Sciences and Technology, Topi 23460, Pakistan

1 Introduction

The issues of security gain broad interests by empowering corresponding algorithms to reveal more fine-grained solutions and make more accurate predictions than the previous arena by using artificial intelligent (AI) and machine learning (ML) (Zhou et al. 2017a; Viganò et al. 2020). Hence, most security researchers devote themselves to review the opportunities and challenges of AI in wireless and/or network security or cybersecurity. Notably, advanced intelligent systems primarily emphasize learning from vast amounts of data with the goals of high efficiency, minimum computational cost, and substantial predictive or classification accuracy (Prasad and Rohokale 2020; Lheureux et al. 2017).

With the recent advancement, AI can boost the performance of security solutions to mitigate the risks from the diverse attacks that we are facing in the field of wireless and/or networking (Lee and Kim 2017; Jiang et al. 2016). The ML techniques, i.e., classification and clustering, are not new, but the importance of these methods can be significantly highlighted in the last several decades (Lin et al. 2019; Larriva-Novo et al. 2020). Previous studies showed that most of the research in security applications used AI to model the attack patterns with their unique features. Nevertheless, the previous studies can be intrinsically weak against new types of high-level attacks with different features. To overcome these limitations of current ML approaches, new techniques must be used to identify diverse security threats and develop more generic and robust security solutions (Bhuyan et al. 2013).

AI/ML can be utilized in numerous applications, such as network intrusion systems, fraud detection, impersonation attack, eavesdropping, spam detectors and scammers. Generally, AI-based solutions work by analyzing huge amounts of data generated by network traffic, host processes and users to detect suspicious activities using efficient algorithms. We envisage that using ML for security applications will become part of the commonly used security techniques very soon. However, these ML-based security solutions might be vulnerable to a new type of sophisticated attack known as adversarial ML (Huang et al. 2011). In many security domains, the attacker can effectively control the information of the input to the ML algorithms to equivocate classifiers designed to distinguish them. Furthermore, the training data set utilized to construct classifiers can be disturbed by adding standard samples to the abnormal sample class and/or vice versa. Threat players are couching the organizations to break their security and disclose users' identification in 5G (Hajoary and Akhilesh 2020). Therefore, it is essential to develop strong security measurements for any system, network or organization (Zou et al. 2016). However, it is important to realize different kinds of security threats and how they work together to break the security measures. Since we are in an era where organizations or businesses will become more digitally advanced than before, the organizations' security strengths must also be improved as the technology improves day by day. In other words, the failure will cause an inflated data break as noticed by different organizations.

Security syndicates several fortifications at the edge or in the network to implement security rules and strategies. In this regard, only authentic devices/users can access the network resources, and malevolent attacks are required to be stopped from misuses and extortions. Furthermore, the world is changed due to digitization, and it impacts our living standards, workplaces, learning abilities, and playing. Therefore, every organization needs to protect its networks and systems from providing reliable services to its patrons. In the recent past, AI has gained popularity in many domains and is now restricted to the computing disciplines. The primary reason for this is the availability of data for

learning purposes in large volumes and variety. This has resulted in AI getting popular, but at the exact time, expectations from AI-based systems are also on the rise. However, a key aspect usually missed out in this context is that the AI can go wrong as well (Winfield 2019). Instead, that can be a perspective development in AI-based systems that can not only go wrong but can be intentionally developed for destruction on a large scale. AI-based security systems are considered one of the significant elements of network security these days. Numerous such systems have been developed with unique techniques to protect networks using an assortment of data-based AI techniques, statistical methods, and ML (Zhou et al. 2017a).

Various proposals have been suggested to tackle security attacks through AI/ML. For instance, the authors of Liu et al. (2021) reviewed and summarized different attacks and defense mechanisms through the deep learning (DL) approach. Since the privacy and security issues of DL can be revealed, the authors also pinpointed the privacy and security issues of the DL approach. Furthermore, the authors of Ni et al. (2021) proposed a service-oriented and location-based efficient key distribution protocol to secure the data transmission. In Dibaei et al. (2020), the authors proposed ML and blockchain as the cybersecurity defense mechanisms in inter-vehicle networking or in-vehicle networking. In Ayodeji et al. (2021), the authors presented a holistic cybersecurity review that demonstrates adversarial attacks against AI applications. Finally, the authors of Jing et al. (2014) analyzed the cross-layer heterogeneous integration and security issues while discussing diverse cryptographic techniques to find out the security solutions in the Internet of Things (IoT).

However, there is still a large room for improvement in these systems to solve the security needs of modern complex software systems in real-world settings. This is because such systems always deal with the massive amount of data that causes slow training and testing processes and can have low detection rates in inappropriate training. All this asks for a single place that summarizes key features, pros, and cons of the existing AI-based security systems. This will not only help in encapsulating the available knowledge in this domain but will also identify avenues of future research. Keeping this in view, this paper provides a detailed overview of various taxonomies and a summary of the exiting AI techniques utilized for security.

1.1 Contribution/summary of the article

First, we categorize and explain distinct aspects of AI that can address wireless network security threats. Although wireless network security threats are well investigated in different attractive directions, we only explore those threats that are solved with the help of AI/ML in Sect. 2. Then, in Sect. 3, we illustrate the lessons learned from the existing techniques and contributions of up-to-date works. Furthermore, we also present several open problems for security measurements that need to be further investigated through AI/ML approaches in Sect. 4. Finally, we conclude our work in Sect. 5. For the background knowledge, we provide appendixes of recent attacks (Appendix 1), security branches (Appendix 2) and security threats (Appendix 3), respectively. The appendixes will help beginners and researchers to work in the direction of security and AI/ML. To the best of the authors' knowledge, this is the first comprehensive survey covering all the security types, threats and proposed AI/ML solutions. For the reader's convenience, the taxonomy of the article is given in the list of contents.

2 Artificial intelligence based solutions

In this section, we highlight the solutions proposed for security threats based on AI/ML. First, we pinpoint all the proposed solutions for communication and network security through AI/ML in Subsection A and B. Then, in Subsection C, we discuss the solutions based on RL for communication and network security. Finally, Subsection D illustrates the deep learning approach to tackle the security threats.

2.1 AI/ML for communication security

The recent progress of users' mobility in the area of communication have demanded higher requirements for the system's reliability and availability (Waqas et al. 2017, 2018b, 2020a). However, the reliability and availability of the system or users' links are further degraded under security threat. Therefore, the overall communication system must detect security threats to achieve data legitimacy and reliability. For this purpose, specific characteristics of users would be employed in temporal and spatial domains. One of the characteristics is the authentication of the wireless channel between users. This channel-based message authentication can be achieved with the help of the ML approach. First, by utilizing ML algorithms, the data from the channel estimations at the receiver end needs to be trained. In this stage, the data also needs to be labelled. The label means that the transmitted signal also requires some cryptographic information to authenticate the sender. In the second stage, the temporal variations of the sender and receiver are considered. Otherwise, it will become impossible to distinguish between the channel's variation and messages introduced by unauthentic users. The overall procedure is summarized in Fig. 1. In this regard, we pointed out several AI-based solutions and summarized them in Table 1.

2.1.1 Identification of unauthentic users

Two prospects can be considered to accomplish the objective of authentication. First, ML algorithms must be frequently updated. Second, the difference between the current and previous states can be utilized as input data for ML algorithms to determine the channel estimation. This helps to detect unauthentic users. Such a kind of approach is proposed

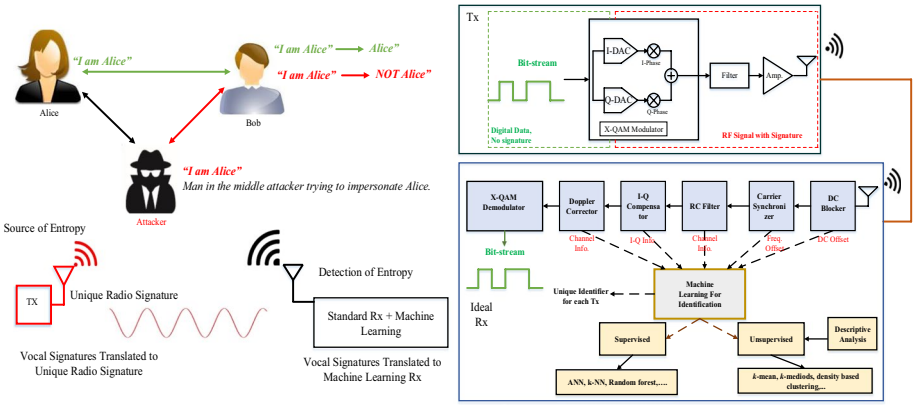

Fig. 1 Machine learning based transmitter identification

Table 1 Machine learning techniques to achieve data and channel authentication in wireless communications

Ref	Year	Scenario	Security threat	Applied technique	Data usage	Achieved goals
Weinand et al. (2017)	2017	Wireless communication	Impersonation detection/ spoofing	Gaussian mixture model	Received data packets from channel estimation	Message authenticity based on physical layer security
Ambekar and Schotten (2014)	2014	Wireless ad-hoc networks				
Pei et al. (2014)	2014	Wireless communication	Impersonation/spoofing	SVM and linear fisher discriminant analysis	Received data packets at receiver	Physical layer authentication
Pan et al. (2017)	2017	Wireless communication	Impersonation/spoofing	ϵ-greedy strategy	Received data packets at receiver	Physical layer authentication
Wang et al. (2017)	2017	Wireless communication	Impersonation/spoofing	Extreme learning machine (supervised learning approach)	Received data packets at receiver	Message authentication/ user authentication
Wan et al. (2017)	2017	Wireless communication	Impersonation/spoofing	Logistic regression/ Frank–Wolfe algorithm	Received data packets at receiver	Reduce communication overhead/user authentication
Xiao et al. (2018a)	2018	Wireless communication	Impersonation/spoofing	Logistic regression/ Frank–Wolfe algorithm	Received data packets at receiver	Reduce communication overhead/user authentication
Bellet et al. (2015)	2015	Wireless communication	–	Logistic regression/ Frank–Wolfe algorithm	Received data packets at receiver	Computational overhead/ communication cost
Blatt et al. (2007)	2007	Wireless communication	Spoofing attack	Incremental aggregated gradient	Gradient values	Logistic regression problem in authentication
Gurbuzbalaban et al. (2017)	2017	Wireless communication	Spoofing attack	Incremental aggregated gradient	Gradient values	Logistic regression problem in authentication
Li and Huang (2018)	2018	Wireless communication	Spoofing attack	SVM algorithm	–	Signal processing strategy to improve the detection of spoofer in the dynamic network

by Weinand et al. (2017), in which the users' channel characteristics is utilized in the frequency domain, i.e., orthogonal frequency-division multiplexing (OFDM). The OFDM channel estimation is used to recognize and validate the channel characteristics. The authors considered sensitive information transmission to pledge information security. The authors utilized the ML approach to train the data from the channel estimation at the received data packets. As a result, the overall performance of the ML approach is better in terms of data detection and false alarm rate. However, the authors did not consider the basic phenomena of the channel detection process: received signal strength indicator, channel state information, or received signal strength and time of arrival to achieve reliable decisions.

Additionally, another critical question is how or whether the message authentication procedure can reduce transmission latency and is essential for system competence. Furthermore, the trade-off between complexity and performance is also one of the important issues when using ML algorithms. In this regard, Ambekar and Schotten (2014) presents different schemes to reduce the errors due to noise in the channel estimation based on preprocessing. In addition, we also need to focus on the users' mobility to validate the threat detection accuracy (Waqas et al. 2018c).

2.1.2 SVM to detect channel features

Taking the above problems of detection and false alarm probabilities, the authors in Pei et al. (2014) proposed two schemes based on different classification algorithms of ML. The authors utilized support vector machine (SVM) based authentication and the linear fisher discriminant analysis based authentication to exploit the channel features, i.e., time of arrival, received signal strength, and cyclic features of a channel. The hypothesis test problem is solved by the linear and nonlinear SVMs based schemes for the performance test. The linear fisher discriminant analysis method is also suggested for a linear combination of channel characteristics to pursue the statistical tests. The statistical tests are estimated with the help of threshold values to implement authenticity. The authors compared different schemes, such as linear SVM, quadratic SVM, polynomial SVM and linear fisher discriminant analysis based schemes to increase detection and decrease false alarm rate probabilities. Through experimental verification, the proposed scheme has been shown to outperform the traditional methods in terms of detection and false alarm probabilities and complexity. However, the proposed scheme did not consider the mobility of users and only considered relatively low, or no mobility scenario (Waqas et al. 2018b).

The works in Pei et al. (2014) and Waqas et al. (2018b) do not talk about the fixed and dynamic threshold value for the detection probabilities and false alarm probabilities. The threshold value has pre-knowledge information about the channel in the previous work. In such a technique, the threshold values due to channel differences are calculated by a system state, interpreted by the ϵ-greedy approach. The ϵ-greedy strategy is utilized to select a threshold value by absorbing the states in previous time slots (Pan et al. 2017). The receiver receives data in every time slots and sets threshold values according to the systems states and gain of the system. Thus, the ϵ-greedy strategy is considered to maximize the optimal threshold value. As a result, the system achieves a better rate of success authentication within 1000 time slots than the fixed threshold value in a dynamic wireless environment.

Another ML-based approach is proposed in Li and Huang (2018) to enhance the accuracy of spoofing detection in the view of low channel stability. The SVM algorithm is applied for the detection process after getting physical layer information. However, the

authors proposed a physical layer authentication (PLA) spoofing detection method based on sparse signal processing to manipulate the sparse representation and the Savitzky-Golay filter. To overcome communication overhead, the authors present a sparse signal processing-based PLA frame to avoid any additional communication overhead. The authors claim that the required method does not require any additional techniques, such as multiple antennas, to detect the spoofing attack. However, the uniformity among authentic users' signals is very low.

2.1.3 PLA hypothesis tests

In several works, the PLA scheme is considered on hypothesis tests to compare channel information with the channel record of the sender to identify the impersonation or spoofing attacks. However, dynamic networks are not always dependent on the hypothesis test because the threshold value in the hypothesis is not always available. Therefore, it is necessary to exploit the multidimensional characteristics of wireless channels. Thereby, we can utilize the generated training data from a model to increase the detection accuracy. Such a scenario is studied in Wang et al. (2017), where the authors apply an extreme learning machine to explore PLA. The authors considered a two-dimensional measure and pseudo adversary model to create training data based on legitimate user's messages. They utilize the ML classifier to attain PLA. The advantages of the multidimensional measure are used to enhance detection performance. In addition, the adversary model is also investigated to achieve the training data for extreme learning machine based authentication through a supervised learning algorithm. PLA techniques using ML is an essential factor in achieving the information, such as received signal strength indicator, received signal strength, channel state information and time of arrival. The information is used to distinguish the wireless transmitter and discover spoofing attacks with lower overhead to achieve integrity, secure communication and authenticity.

2.1.4 Logistic regression-based authentication

The same problem of a hypothesis test for spoofing detection in the PLA is also considered in Wan et al. (2017) and Xiao et al. (2018a). For this purpose, the authors proposed logistic regression-based authentication to eliminate the assumption on the known channel model with the help of multiple antennas. The authors explored multiple stations at different locations to estimate channel information. This approach can increase the spatial resolution of the wireless channel regarding the transmitter. Thus, the PLA system can exploit multiple stations with multiple antennas to improve spatial resolution by increasing the accuracy of spoofing detection. The Frank–Wolfe algorithm can also be used to evaluate the parameters of regression-based authentication (Jaggi 2013). Furthermore, the constant is estimated under the 1-norm constraint in the Frank–Wolfe algorithm to limit complexity and compromise the trade-off between the regression testing and training errors.

However, the Frank–Wolfe-based PLA requires the channel information from transmitter to receiver. Therefore, the PLA with multiple landmarks can also be applied as a distributed Frank–Wolfe algorithm to resolve convex optimization problems of the Frank–Wolfe algorithm in a distributed manner. The advantage of distributed Frank–Wolfe based PLA increases the convergence rate. It can also reduce computational overhead and communication cost after each iteration in a distributed way (Bellet et al. 2015). Therefore, the PLA based models can calculate the channel information on multiple antennas at the diverse

locations to identify the spoofing attack in a precise manner. The distributed Frank–Wolfe based PLA recalculates the gradients of entire training data in each iteration, which results in large computation overheads and latency problems. Thus, an online technique known as the incremental aggregated gradient is proposed in Blatt et al. (2007) and Gurbuzbalaban et al. (2017) to solve regression-based authentication problems. In incremental aggregated gradient-based PLA, the tasks are managed in a deterministic order, and the previous gradient values can be utilized to increase the convergence rate. It is concluded in Blatt et al. (2007) and Gurbuzbalaban et al. (2017) that distributed Frank–Wolfe based PLA can accomplish better accuracy to discover spoofing attacks while reducing communication overhead. Contrarily, the incremental aggregated gradient-based PLA can reduce the computational overhead and obtain a higher detection precision.

2.1.5 Authentication of IoT wireless devices

Authentication of IoT devices in wireless communication is another important factor. Specifically, the traditional authentication in wireless communication systems protects the data within networks via diverse techniques, e.g., digital signatures and hash-based message authentication codes. However, such techniques normally cannot address key recovery attacks and brute force attacks. Furthermore, an open authentication protocol (OAuth-P 2.0) (Chatterjee et al. 2019) shows that such techniques are not able to prevent an adversary from replication or secret modelling identification of encrypted keys and channel information.

Thus, OAuth-P is also susceptible to cross-site-recovery forgery (Yu et al. 2012). Another protocol called physical unclonable functions can leverage robust and secure at low-cost system (Yu et al. 2012; Roel 2012). Taking the motivation from human communication to utilize intrinsic differences in voice signatures to detect a particular speaker, the radio frequency - physical unclonable function permits real-time verification of wireless users based on deep neural networks (DNN) (Kömürcü and Dündar 2012; Chatterjee et al. 2019). A physical unclonable function that uses the radio frequency properties of transmitters and the receivers to detect the variation over in-situ ML technique. The best thing in this process is that the proposed method does not rely on any additional circuitry but utilizes the current asymmetric radio frequency communication framework. In addition, the overload of the device authentication is entirely moved to the gateway receiver.

IoT systems can considerably benefit from physical unclonable functions based authentication protocol. The physical characteristics of the transmitter would be examined and stored in a protected server as a common practice in IoT to replenish the traditional secret-key based authentication scheme. In Xu et al. (2020), a comprehensive survey of the contribution of AI to IoT security in edge computing is presented. The authors also discussed the survey of privacy preservation and blockchain for edge-enabled IoT services with AI.

2.2 Machine learning for network security

The technology is getting mature in almost every area such as finance, economics, medical science, engineering, and social science due to the rapid development of IoT, cloud computing, and big data (Ahmed et al. 2018b; Zeng et al. 2018). However, the data exploration techniques cannot meet the requirements, optimization, and fast network security. Thus, it is paramount to use comprehensive optimization techniques to accomplish data analysis and prediction/detection in network security (Dai et al. 2019). Therefore, prediction

becomes an imperative subject to be explored. The procedure of network security to detect the malicious users and apps are shown in Fig. 2. Taking the network security into consideration, the authors in Gu and Li (2016) propose SVM to detect security threats in networks. Furthermore, the authors analyze diverse kernel functions instead of a single kernel function to prevent any imperfection in learning and generalization capability to develop SVM kernel functions. For this purpose, the authors proposed a model based on multi-combination forecasting. The method is to take joint decisions on the results while eluding the insistence of a single prediction model. Hence, the predictions become more accurate. Moreover, particle swarm optimization algorithms can also be applied for the optimization of SVM parameters. Consequently, the procedure of SVM optimization is precise and avoids the issues of convergence to detect network security. In this regard, we pointed out several AI-based solutions and summarized them in Table 2.

2.2.1 Reliability and security

The recent advancement of IoT and cyber-physical systems (CPS) has imposed extreme reliability and security challenges (Chen et al. 2018b). This is due to the heterogeneity and multifarious connectivity of the CPS components as well as the erring and vulnerable nature of the underlying devices, abrasive operating environments and increasing security threats (Chen et al. 2011). The diverse reliability threats can pose different challenges that lead to numerous mitigation techniques on different layers. Therefore, it is necessary to take good care about the safety and security of ML algorithms before exploiting any ML-based security measures. The reason is that there are a large number of devices in IoT networks (comprising of sensors and actuators) linked together over wired or wireless networks. For this massive group of devices, security is identified as the weakest area. Therefore, researchers are trying to focus on authentication and access control in the IoT. However, the important thing is to secure the entire system. Therefore, the authors in Xiao et al. (2016b) tried to pinpoint the security challenge using ML within IoT gateways to secure the whole system. For this purpose, the authors utilized two ML approaches, i.e., artificial neural networks (ANNs) and genetic algorithms. The ANNs mime the neurons and organic processes within the brain to transfer information for communicating, learning, and decision-making (Tu et al. 2020b). Similarly, the ANN can be used in an IoT network to supervise the state of IoT devices and to make communication decisions.

2.2.2 Securing network sensitive data

Any information and event management system must normalize security threats employing preventive technologies in an enterprise. The experts of the security operation center need to explore truly malicious attacks for security alerts. Mostly, the alerts are irresistible, and most of these alerts are false positives. Therefore, it is difficult for security operation centers to handle all these alerts at once. Consequently, potential attackers can attack and compromise the host. In this regard, ML is a feasible methodology to decrease the false positive rate and increase the productivity of security operation center experts. Keeping this in view, the authors in Feng et al. (2017b) developed a user-centric ML frame. They considered data sources in the security operation center by leveraging and processing data sets to propose an efficient ML system.

Furthermore, to efficiently detect network intrusion, we need to gather a large sum of sensitive information. Thus, we need to assemble several transactions detail from the

Table 2 Machine learning techniques to detect malicious attack in network/cyber security

Ref	Year	Scenario	Security threat	Applied technique	Data usage	Achieved goals
Gu and Li (2016)	2016	Network security	–	SVM/Particle swarm optimization algorithm	Kernel function	Prediction accuracy
Chen et al. (2011)	2011	IoT/CPS	–	–	–	To secure ML algorithms
Xiao et al. (2016b)	2016	IoT	–	ANN and genetic algorithm	–	Communication, learning and decision making for IoT devices
Feng et al. (2017b)	2017	Security operation center	Malicious attacks	Centric ML framework	Data sources	Reduce false positive rate
Aljawarneh et al. (2018)	2018	Network intrusion	Intruders	J48/Meta Pagging, Random Tree, REPTree, AdaBoostMI, DecisionStump and NaiveBayes	Network transactions data	High false and low false negative rates accuracy
Aljawarneh et al. (2018)	2018	Network intrusion/cyber attack	DoS, command Injection and malware	Deep multilayer perception/RNN	–	To improve the detection latency
Narudin et al. (2016)	2016	Cybersecurity	Malware attack	Naive Bayes, Multi-layer perception, decision tree, K-nearest neighbor and Random Forest	Set of files	Detection rate accuracy (information, contents, time and connections)
Han et al. (2016)	2016	Cloud Computing	Co-resident attack	Semi-supervised learning approach	–	To identify the behavioral differences between attackers and normal users

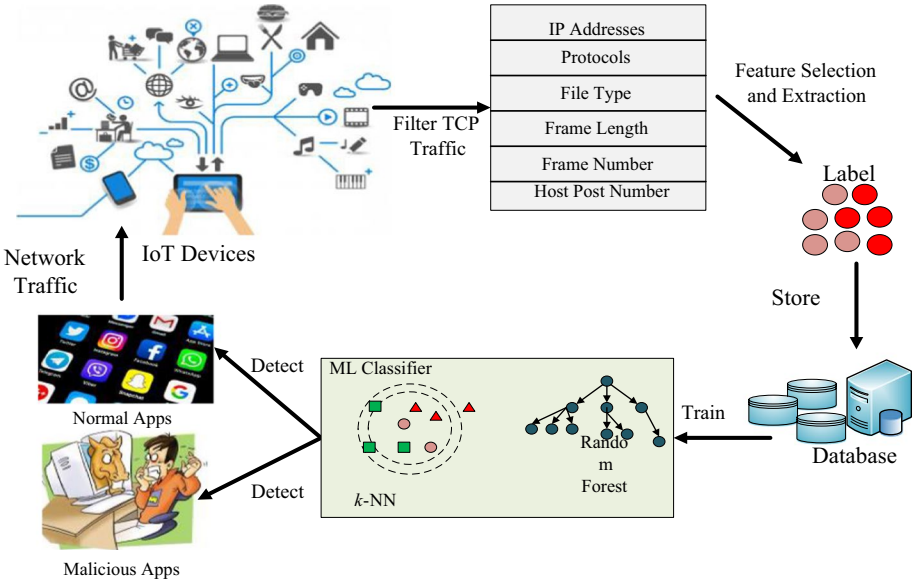

Fig. 2 Machine learning based network detection

network (Otoum et al. 2019). To examine fake network transactions, the estimation of intruder's data is essential, based on meta-heuristic irregularity. Furthermore, fake transaction identifications are necessary to construct and provide predictions related to the intrusion possibility based on the accessible attribute aspects. The authors in Aljawarneh et al. (2018) developed a hybrid model to estimate fake transactions by using the network transaction data as training data for ML algorithms. In this regard, the transaction data is filtered with the help of the voting algorithm. For data classification, the authors utilized J48, Meta Tagging, Random Tree, REPTree, AdaBoostM1, DecisionStump and NaiveBayes. These classifications showed that most of the attacks in the network occur using transmission control protocol (TCP).

2.2.3 Deep multilayer perception and RNN

The intrusion attack is also an attracting interest (Waqas et al. 2020b). The problem of exploiting ML is typically affording limited processing resources and thus, most of the solutions are rule-based or lightweight ML practices. Accordingly, the computational offloading for resource-constrained mobile devices must be taken into consideration. For this purpose, the authors in Aljawarneh et al. (2018) studied a case for a small four-wheel robotic vehicle. They validated the particularity and advantages of offloading the continuous tasks by exploiting DL for intrusion detection. Both deep multi-layer perception and recurrent neural network (RNN) architectures were utilized to prove the learning of different attacks. The different attacks include DoS, command injection, and malware for cyber-attacks for a robotic vehicle. A mathematical model is also developed to detect latency for computation offloading and processing requirements for DL. The authors concluded that more dependable network and processing requirements reduce the detection latency by achieving offloading.

2.2.4 Securing sensitive data

Moreover, hackers can increase the number of malicious attacks proportional to the number of users. Users have their sensitive data available on their devices, and it is not taken care of in terms of security. Therefore, we cannot rely on the current approaches as it is not sufficient to handle the malware detection. Thus, we need to propose an alternate solution to evaluate malware detection. For instance, the authors utilized an anomaly-based approach with ML classifier in Narudin et al. (2016). The authors considered four categories in this work, such as basic information, contents, time, and connection. The ML classifier is utilized to improve the malware detection for massive data files and obtained an optimal classifier to distinguish mobile malware. The classifiers comprise the Bayes network, multi-layer perception, decision tree, k-nearest neighbor, and random forest. Among different algorithms, the highest accuracy, i.e., 99% were indicated by a random forest classifier. The K-nearest neighbor classifier also showed 84% correctness for malware detection. Hence, the authors prove that ML classifiers can detect malware attacks. However, it is noted that excessive processing is required for having a larger dataset, but it will increase the precision.

2.2.5 Semi supervised learning

The real-time malware detection exploiting ML classifiers also needs investigation. One of the suggestions is the cloud-based scenario because the approach is effective in the ML technique for a real mobile malware environment. Keeping this point in view, the authors in Han et al. (2016) focus on co-resident attacks in cloud computing by exploiting a semi-supervised learning approach. The authors focus on the risks at the virtual machine level and co-resident attack. In the co-resident attack, the attacker can get sensitive information from virtual machines that co-locate on the same server. Therefore, the authors proposed a defense mechanism against the co-resident attack in the cloud computing environment. Techniques such as clustering and semi-supervised learning are used to recognize the behavior between attackers and normal users. Consequently, the attackers are forced to perform as legal users because virtual machines (belonging to the same users) can co-locate each other. In this way, the attacker's cost is increased, but in practice, there is also a cost of launching virtual machines. Another limitation of this work is that the defense mechanism is only for a single data center. However, the size of the data center also influences the probability of co-location. Therefore, it is necessary to organize the defense mechanism across multiple data centers.

2.3 Reinforcement learning approaches

Wireless communications are susceptible to different threats, e.g., spoofing or impersonation attacks. In such attacks, the impersonator can claim to be a legitimate node by impersonating a fake identification (Tu et al. 2021). In this way, an impersonator will easily attain illegal advantages to perform MITM and DoS attacks. In order to cope with this challenge, the PLA technique can be applied. The PLA scheme leverages physical layer characteristics of the wireless channel to reveal impersonation attack/spoofing attack (Tello-Oquendo et al. 2018; Tu et al. 2018c). The properties of PLA consist of received signal strength, channel impulse response, received signal strength indicator, channel state information,

and channel frequency response (Liu et al. 2013, 2014; Tugnait 2013; Jiang et al. 2013). These properties can be utilized to reveal an impersonation attack. However, there are certain problems in channel responses due to wide-band wireless communication. One of the specific challenges is that a wireless channel is not static, and the channel characteristics change dynamically. Therefore, it is difficult to predict a spoofing/impersonation attack. For instance, the spoofing detector in Xiao et al. (2007) differentiates the transmitters at diverse places, due to which a hypothesis test equates the channel frequency response with the media access control (MAC) addresses. Thus, the precision of PLA spoofing detection can be performed at the receiver that relies on the threshold test of the hypothesis test. Again, there is an issue of test threshold because it becomes difficult for the receiver to choose an appropriate threshold value for spoofing detection without considering the values of channel parameters, especially in a dynamic environment. In this regard, we pointed out several RL based solutions and summarized them in Table 3.

The users as well as attackers are independent and have flexible control over the transmission. Thus, conventional methods, such as game theory (Conley and Miller 2013), have shown strengths to improve security, but they are primarily applicable in a static environment. Therefore, in RL methods, i.e., Q-learning, deep Q-Network (DQN) and Dyna-Q, a user can attain an optimum approach in a dynamic environment without considering the system's information as illustrated in Fig. 3. Other approaches, such as channel selection strategy with Q-learning in Conley and Miller (2013) discourse jamming attacks and the channel retrieving with Q-learning in Gwon et al. (2013), have investigated the jammers in a hostile environment. In addition, Dyna-Q can increase the learning speed by employing the hypothetical understandings (Sutton and Barto 1998). In order to compare game theory and RL techniques, the authors in Xiao et al. (2015, 2016a) investigate the PLA in dynamic wireless networks. They compare channel state information of the data packets to identify spoofing attacks by the zero-sum game and Q-learning and Dyna-Q. The authors proposed the PLA algorithm by leveraging channel state information to find out the test threshold by using RL without knowing the complete information of the channel, such as channel condition and time variation. However, the optimal test threshold in the hypothesis test is attained by trial and error to exploit PLA efficacy. The experimental results with the zero-sum game, Q-learning and Dyna-Q showed that the spoofing detection is robust against environmental variations. However, among them, Q-learning can improve authentication performance. In addition, the spoofing detection technique with Dyna-Q improves the learning speed of Q-learning and, hence, improves the performance. However, the limitation of these works is that the PLA is incorporated with traditional authentication schemes at MAC and network layers. For instance, packets acknowledged by PLA can be further authenticated at MAC protocol.

Game theory is also an influential mathematical tool for a security mechanism to examine the connections among different players for diverse goals (Chen et al. 2011). A simple example is a communication between a spoofer and a legitimate user that achieves the channel based spoofing detection (Xiao et al. 2016a). In the formulation, the receiver selects its test threshold to increase the payoff, and the spoofer chooses the transmission of spoofing signals. The works in Xiao et al. (2015, 2016a) are further extended to the MIMO system by formulating a channel based MIMO authentication game in Xiao et al. (2016b, 2017). In this work, a spoofer selects its attack rate in the game. It means that a spoofer transmits a spoofing signal to increase its utility based on Bayesian risk. The receivers determine the test threshold according to the number of antennas and sample size of frequencies. It is shown that the threshold test increases with the number of antennas to avoid discarding the authentic signals and consequently

Table 3 Reinforcement learning approaches to secure channel authentication and detect jamming and eavesdropping attacks

Ref	Year	Scenario	Security threat	Applied technique	Data usage	Achieved goals
Xiao et al. (2007)	2007	Network layer	Impersonation	Q-Learning	MAC addresses	Physical layer authentication
Conley and Miller (2013)	2013	Hostile environment	Jamming attack	Q-Learning	Hypothetical experiences	Channel authentication
Gwon et al. (2013)	2013	Hostile environment	Jamming attack	Dyna-Q	Hypothetical experiences	Increased learning speed of RL algorithms for detection rate
Xiao et al. (2015, 2016a)	2015, 2016	Dynamic wireless networks	Impersonation	Dyna-Q	data packets	To achieve test threshold without knowing the complete information of channel condition and time variation.
Xiao et al. (2016b, 2017)	2016, 2017	MIMO environment	Impersonation	Q-Learning	–	To distinguish fake and real transmitters
Moore and Atkeson (1993)	1993	MIMO environment	Spoofing	Dyna-PS	–	Fast learning rate and higher detection accuracy
Xiao et al. (2018b)	2018	NOMA transmission	Jamming attack	Dyna-Q learning	–	To accelerate the learning speed of the Q-learning based power allocation
Xiao et al. (2018c)	2018	Underwater acoustic network	Jamming attack	Deep Q-network	–	To achieve fast learning, higher SINR and lower bit error rate
Chen et al. (2018a)	2018	Wireless body area network	Jamming attack	Deep Q-network	–	To resist the jamming attacks from WBANs
Xiao et al. (2018d)	2018	DQN based mobile communication	Jamming attack	Deep CNN and macro-action technique	–	To develop two-dimensional anti-jamming communication and user mobility to address jamming and interference
He et al. (2016)	2016	Energy harvesting comm. / cognitive radio/cloud system	Jamming attack	minimax post-decision state and win-or-learn fast post decision state	–	To enable the legitimate system to learn and adapt faster in a dynamic environment

Table 3 (continued)

Ref	Year	Scenario	Security threat	Applied technique	Data usage	Achieved goals
Amuru et al. (2016)	2016	–	Jamming attack	MAB framework	–	To learn the optimal attack strategies against both static and adaptive victim transmitter/receiver

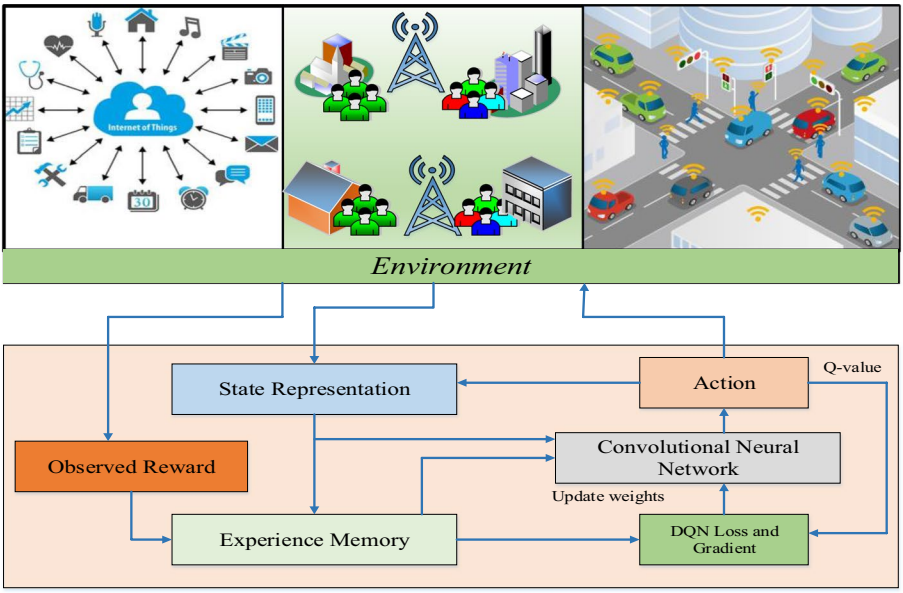

Fig. 3 Reinforcement learning procedure to detect malicious users

decreases the attack rate. The authors also explore the dynamic MIMO authentication game by exploiting the received signal strength indicator at the receiver end to distinguish the transmitters without considering the channel time variations and authentication costs in each time slot. For this purpose, the receiver employed RL algorithms to acquire optimal test threshold with spoofer interaction and the unknown MIMO environment. However, the performance is further investigated by Dyna architecture and prioritized sweeping (Dyna-PS) (Moore and Atkeson 1993). The Dyna-PS based spoofing detection established a learned model to implement the detection schemes in MIMO systems. It is stated in Moore and Atkeson (1993) that the performance of Dyna-PS exceeds the Q-learning scheme with a faster learning rate and high detection precision.

The authors in Xiao et al. (2018b) also proposed RL based power control technique for the downlink non-orthogonal multiple access (NOMA) transmission without the awareness of jamming and radio channel parameters. The zero-sum game is formulated for the power allocation of the base station in a NOMA system furnished along multiple antennas competing with an intelligent jammer. Here, the base station is the leader that initially selects the transmission power of multiple antennas. The jammers act as the followers that choose the jamming power to disturb the transmission. The Dyna architecture is also utilized to formulate the methods. It manipulates the experiences to set the values that are used to quicken the learning speed. Hence, it improves the communication of the NOMA transmission in the presence of smart jammers. In short, the Q-learning based power allocation method is applied for multiple users in the dynamic NOMA transmission against smart jammers without being conscious of the jammers and channel models. Further, the Dyna architecture and hot-booting schemes are utilized to speed up the learning rate to develop the anti-jamming NOMA communication.

2.3.1 DQN techniques

As the above discussion, the anti-jamming transmission framework is considered in the underwater scenario in Xiao et al. (2018c). The RL is applied to regulate the power transmission. This work finds mobility to challenge the jammers in underwater acoustic networks. However, the authors considered the deep Q-networks based transmission without considering the jamming and underwater channel model. In this technique, the underwater transmitting transducer utilizes the DQN to choose the power transmission according to the transmission state. It involves SINR and received signal strength indicator of the acoustic signals. The receiver also applies DQN to select the changing position to fight strong jammers based on the last transmission performance and the mobility cost. The experimental results verify that Q-learning has a high learning speed and SINR, a lower bit error rate of the signals, and higher utility. The same technique is also used for another application, i.e., wireless body area networks (WBANs), to report the jamming attacks for supporting health care (Chen et al. 2018a). The same RL based power control scheme is adapted to communicate between the in-body sensors and the WBAN coordinators to stop jamming attacks.

More specifically, the Q-learning scheme is applied to guide the coordinator to achieve a power control scheme without knowing the parameters of the in-body sensor's transmission and the WBANs model of the other sensors for anti-jamming. However, the transfer learning technique is applied to increase the learning rate instead of DQN while considering Stackelberg game theory. The jammers can dynamically change the jamming strategy based on security approaches by using smart radio devices. It also encourages mobile devices to enter an exact communication mode and then introduce the jamming procedure consequently. However, the users use spread spectrum and mobility to tackle both jamming and interference. Thus, the authors in Xiao et al. (2018d) proposed a two-dimensional anti-jamming mobile communication method. They applied the RL to attain an optimal communication strategy without knowing the jamming, interference, and channel model. DQN based two-dimensional mobile communication structure can be utilized to decrease the exploration time at the beginning of the game. For accelerating the learning in a dynamic situation, the deep convolution neural networks (deep CNN) and macro-action technique can be applied to improve a two-dimensional anti-jamming communication to tackle jamming and interference.

The RL algorithms do not provide any guarantee for the jammer actions and are computationally complex. Therefore, the learning-based algorithm, called multi-armed bandit (MAB) framework is described in Amuru et al. (2016), to enable the jammer and learn the optimal physical layer jamming policy. In contrast, the MAB algorithm enables the jammers to discover the attack schemes against the transmitter-receiver pair by concurrently selecting the actions from both finite and infinite arm sets. In MAB, the jammer can select several physical layer features, i.e., signalling scheme, power level and on-off/pulsing duration, to attain the jamming approaches.

The major disadvantages of most of the RL algorithms are the prior information of jammers about the tactics used by transmitter-receiver pairs, the channel gains, channel state information etc. that might not be applicable for practical scenarios (Amuru and Buehrer 2014). It is also concluded in Amuru and Buehrer (2014) that it is not always necessary to get the optimal solution to match the jammer's signals to the victim's signalling as the optimal jamming signal follows a pulsed jamming approach. Nevertheless, these optimal jamming policies are achieved by assuming the prior information

regarding transmitter-receiver pairs. Therefore, it is necessary to develop online learning algorithms that learn the optimal jamming strategy by communicating to transmitter-receiver pairs. Especially, the jammers need to learn to perform in an unknown environment and maximize the total rewards in terms of jamming success rate.

2.4 Deep learning (DL) approaches

The popularity of wireless connectivity is increasing, and network providers are craving for best solutions from the beginning for 5G networks. Therefore, it is necessary to focus on security to tackle security threats, such as protecting users, protecting network equipment, protecting data from malicious attacks, unauthorized access, and data leakage. Conversely, cyber-security systems need to protect mobile devices and users through intrusion detection systems, anti-virus software, and firewalls (Buczak and Guven 2016; Tu et al. 2020a). A firewall is the security defense mechanism based on predefined rules to permit or block the uplink and downlink data traffic. In addition, some anti-virus software can identify and eliminates viruses, worms and trojans, and malware from computers. Finally, IDS detect non-legitimate and malicious activities and violation rules in the information system. Each identification can perform its function to defend communication, servers and edge devices.

Nowadays, DL has an essential role in cyber-security systems (Kwon et al. 2017). DL has various advantages in security. For instance, it automatically learns the signatures and patterns from experience and generalizes them to future intrusion through supervised learning. Furthermore, based on unsupervised learning, it can also detect patterns that are different from the regular behavior of the attackers. Thus, DL can considerably alleviate the effort to redefine the rules for distinguishing intrusions. However, attackers can also use DL to bring a wide range of potential in stealing and cracking users' passwords or private information. Thus, we discuss DL driven network security from three diverse perspectives, i.e., infrastructure security, software-level security and traffic analysis. In this regard, we pointed out several DL based solutions and summarized them in Tables 4 and 5. Moreover, the procedure of DL is also shown in Fig. 4.

2.4.1 Infrastructure level security

The infrastructure level security works on detecting inconsistencies in the physical system. In this level of security, we mainly focus on anomaly detection, which is not conformed to likely behaviors, such as detecting network events, including attacks, random access, and data usage. Researchers are exploiting the unresolved unsupervised learning ability of auto-encoders in this regard (Yousefi-Azar et al. 2017). In addition, researchers are investigating different features of attacks and threats in the existing IEEE 802.11 networks (Thing 2017). In Thing (2017), the authors employed a stacked auto-encoder to classify the network traffic into five categories, i.e. legitimacy, flooding, injections, and impersonated traffic and achieved 98% accuracy. The auto encoding method is also proposed in Feng et al. (2017a) for multi-layer perceptron and stacked auto-encoder for feature selection, extraction, indicating effective implementation.

Likewise, the auto-encoders are also utilized to detect abnormal spectrum usage in wireless communication (Khan et al. 2016). The authors claimed that the detection accuracy could considerably benefit from the depth of auto-encoders. Another issue is the distributed attack detection in the network, which is of utmost importance in wireless security. For instance, the authors in Khan et al. (2016) focused on detecting flooding attacks in

Table 4 Deep learning approaches to achieve detection accuracy of malicious users

Ref	Year	Scenario	Security threat	Applied technique	Data usage	Achieved goals
Buczak and Guven (2016)	2016	Intrusion detection system	Virus/unauthorized access and data leakage	Deep learning	–	To identify and eliminates viruses, worms, trojans, and malware from computers
Kwon et al. (2017)	2017	Cybersecurity systems	Stealing and cracking user's passwords or information	Deep learning	–	To alleviate the effort of pre-define rules for distinguishing intrusions
Thing (2017)	2017	IEEE 802.11 networks	Legitimacy, flooding, injections and impersonation	Stack auto encoder	–	To achieve detection accuracy
Feng et al. (2017a)	2017	IEEE 802.11 networks	Traffic impersonation	multilayer perceptron and Auto encoder	–	To achieve feature selection, extraction, indicating significant implementation
Khan et al. (2016)	2016	Wireless mesh networks	Flooding attack	Auto encoder	100 users (injecting artificial distributed flooding attacks)	To detect abnormal spectrum usage in wireless communication
Diro and Chilamkurti (2018)	2018	IoT environment	–	Deep learning	–	To detect diverse distributed attacks in IoT environment
Saied et al. (2016)	2016	IoT environment	DoS attacks	multilayer perceptron	Patterns of attack occurrences	To distinguish distributed DoS attacks by exemplifying the typical patterns of attack occurrences
Martín et al. (2017)	2017	IoT environment	–	Variational auto encoder	Patterns of attack occurrences	Detection of intrusion occurrences
Hamedani et al. (2018)	2018	Delayed feedback network	Malicious attacks	multilayer perceptron	–	Detection of malicious attacks
Tam et al. (2017)	2017	Mobile networks	Malware and botnets	Deep learning	–	Detection of malicious attacks on users' device

Table 4 (continued)

Ref	Year	Scenario	Security threat	Applied technique	Data usage	Achieved goals
Yuan et al. (2014)	2014	Android mobile users	Malware attack	Training of RBM	300 samples	Improvement of detection accuracy
Yuan et al. (2016)	2016	Droid detector	–	Deep learning	–	Improvement of detection accuracy
Su et al. (2016)	2016	Android applications	Malware attack	DGNs	previous intrusion occurrences	Improvement of detection accuracy
Hou et al. (2016)	2016	Android applications	Malware attack	Deep4MalDroid	–	Detection of Android malware accurately
Martinelli et al. (2017)	2017	Mobile Network	–	CNN	Syscall traces	To identify the sequences of opcodes in order to indicate the malware

Table 5 Deep learning approaches to achieve detection accuracy of malicious users

Ref	Year	Scenario	Security threat	Applied technique	Data usage	Achieved goals
McLaughlin et al. (2017)	2017	Mobile network	Malware attack	CNN	Byte-code text	To draw the inspiration of NLP
Chen et al. (2017)	2017	–	Malware attack	RBM	–	Feature extraction and classification of malware attacks
Rodríguez-Gómez et al. (2013)	2013	Mobile network	Botnet	Deep learning	–	Detection of botnets attack
Oulehla et al. (2016)	2016	Mobile network	Botnet	ANN	–	To identify both client-server and hybrid botnets to demonstrate positive performance
Torres et al. (2016)	2016	Mobile network	Botnet	Long short term memory	Botnets patterns	To employ under-sampling as well as over-sampling techniques to address the class inequity between botnet and common traffic
Eslahi et al. (2016) and Alauthaman et al. (2018)	2016, 2018	Mobile network	Botnet	Multilayer perceptron	Botnets patterns	To perform mobile and peer-to-peer botnet detection by getting high accurateness, respectively
Gwon and Kung (2014)	2014	Traffic identification in network	–	DL-based flow inference technique	Data packets patterns	Flow inference is attained by utilizing and analyzing MAC layer parameters as well as TCP/UDP/IP flow
Wang (2015)	2015	Traffic identification in network	–	ANN	TCP sessions bytes	Traffic identification form traffic monitoring attack
Lotfollahi et al. (2017)	2017	Traffic identification in network	–	Deep packet scheme	Spotify and Bit Torrent	To achieve precision for traffic type classification and accuracy for application type classification

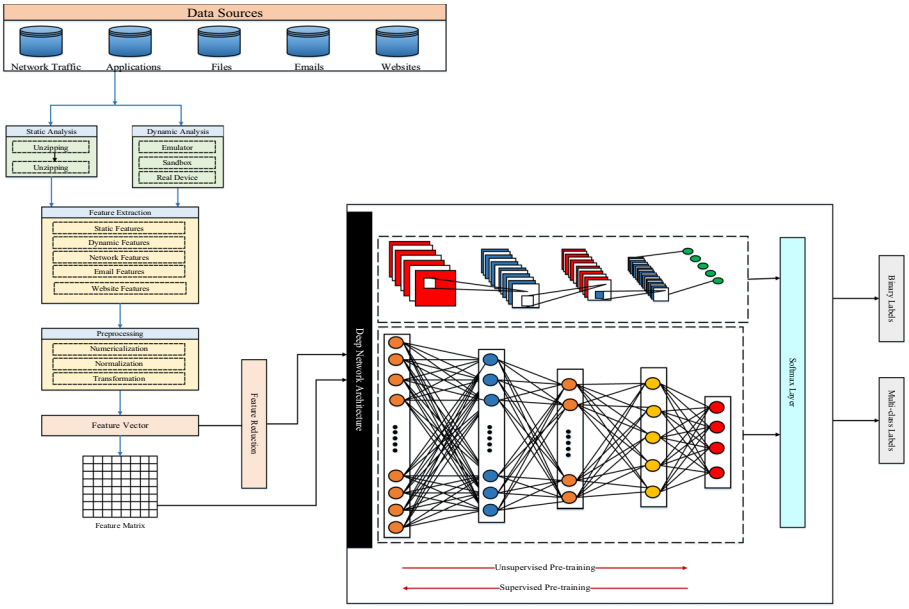

Fig. 4 Deep learning procedure to detect malicious attacks

wireless mesh networks. They analyze their simulation results with 100 users in the wireless environment by injecting artificial and severe distributed flooding attacks to make a synthetic data set. The results show false negative as well as false-positive rates based on the DL approach.

In Diro and Chilamkurti (2018), the authors proposed the DL in an IoT environment to detect diverse distributed attacks. The work in Saied et al. (2016) also exploits multi-layer perceptron to distinguish distributed DoS attacks by exemplifying the typical patterns of attack occurrences. The proposed model is beneficial in terms of detecting both known and unknown DDoS attacks. For IoT environments, the authors in Martín et al. (2017) proposed a conditional variational auto-encoder to detect the intrusion occurrences. They suggested that the variational auto-encoder infers the missing characteristics related to imperfect measurement to increase the detection performance. The factual data descriptions are implanted into the decoder layers to support the final classification. In another work Hamedani et al. (2018), a multi-layer perceptron to identify malicious attacks in the delayed feedback networks was proposed. The authors achieved 99% accuracy in results over 10,000 trials.

2.4.2 Software level security

The software level work is centered on detecting malware and botnets in mobile networks. Currently, mobile devices are carrying a substantial amount of private information. Private information might be stolen and misused by malicious applications installed on smartphones for impractical purposes (Tam et al. 2017). DL can be utilized to analyze and detect such kinds of malicious attacks. In this regard, the authors in Yuan et al. (2014) used both labelled and unlabeled mobile applications to train restricted Boltzmann machine (RBM). The proposed model classified Android

malware detection with remarkable accuracy by learning 300 samples. It also outperformed almost 19% from traditional ML tools. The authors in Yuan et al. (2016) further investigated Droid detector to improve the detection precision by 2%. Furthermore, Su et al. (2016) analyzed the essential features of Android applications, i.e., request permission, user permission, sensitive applications programming, and call interface by using DL. The authors employed deep grid networks (DGNs) to extract the features of malware attacks and proposed SVM for classification. The results show that by using DL, they achieved high accuracy and required only 6 seconds per intrusion occurrence.

The malware detection problem is also investigated in Hou et al. (2016) by pointing out signature-based detection to deal with sophisticated Android malware. The authors proposed a component traversal technique to address the problem. The component traversal technique automatically executes code routines to construct weighted directed graphs. The authors in Hou et al. (2016) also proposed a framework called Deep4MalDroid by leveraging stacked auto-encoder to detect Android malware accurately. This work is further investigated in Martinelli et al. (2017) by exploiting CNNs to discover the relationship between application types and extracted syscall traces from real mobile devices. The CNN technique is also used to draw the inspiration of NLP and take the disassembled byte-code of an application as a text for analysis in McLaughlin et al. (2017). The authors demonstrated that CNNs could efficiently learn to identify the sequences of opcodes to indicate the malware. The authors in Chen et al. (2017) incorporated the location information into the detection framework by exploiting an RBM for feature extraction and classification. The proposed technique improved the performance as compared to other ML methods.

In mobile networks, Botnet is another crucial threat. A Botnet is an effective network that includes machines that are compromised by bots. Such kinds of machines are usually under the control of botmasters. Botmasters take advantage of the bots to harm public services, and systems (Rodríguez-Gómez et al. 2013). The detection of these bots is one of the challenging and pressing tasks in cyber-security. DL also plays a vital role in this regard. For instance, the authors in Oulehla et al. (2016) suggested neural networks extract features from mobile Botnet behaviors. The authors designed an equivalent detection framework to identify both client-server and hybrid botnets to demonstrate positive performance. In Torres et al. (2016), the authors examined the common behavior patterns of botnets to exhibit across the life cycle by using long short term memory. They employed under-sampling and over-sampling techniques to address the class inequity between Botnet and expected data set data. It is also common in irregularity detection problems. Similar problems were also investigated in Eslahi et al. (2016) and Alauthaman et al. (2018), where the authors used standard multi-layer perceptron to perform mobile and peer-to-peer botnet detection by getting high accurateness, respectively.

Although most DL based solutions focus on the existing network attacks to tackle different problems, new attacks are emerging every day. These new attacks have different features and appear in normal behavior. Therefore, conventional NN models cannot quickly identify these tricky attacks. Thus, an efficient DL mechanism must be used to transfer the knowledge of old attacks to identify newer attacks. Moreover, DL approaches should understand the features of unknown attackers and update the underlying model persistently. For this purpose, transfer learning and lifelong learning are two effective techniques for overcoming such problems.

2.4.3 Traffic analysis

The main issues for cyber-security are traffic inference. In order to process the decision making of traffic inference, it requires the analysis of a large number of network features and notions towards the attack-related features. The objective of flow inference is to describe the original flow features generated at the transmitter according to the packets received by the receiver. Therefore, it is critical for intrusion detection, traffic monitoring, as well as for queue management. To identify the traffic, an easy method is to classify the traffic by the port numbers. However, this method is not efficient because many applications (for instance, P2P traffic and video calls) may require a port number initially assigned to other traffic types. To avoid these port numbers, other efficient methods are needed to distinguish between traffic types. In recent years, traffic identification techniques are adopted by utilizing statistical models, or ML (Mao et al. 2018; Draper-Gil et al. 2016). These techniques have been studied to find out traffic features, i.e., the time interval between packets and packet size, are exploited to analyze the types of traffic. However, the patterns of the received flows may have nonlinear variations due to the intricacy of the networks. Consequently, it makes the flow inference very challenging. In this regard, the authors in Gwon and Kung (2014) proposed a DL-based flow inference technique to classify the received packet patterns and assumed the original properties, such as burst size and inter-burst gap.

However, it should be noted that the flow inference is attained by utilizing and analyzing MAC layer parameters and TCP/UDP/IP flows. The inference system is comprised of two layers, i.e., feature extractor and classifier, which are not dependent on each other. The sparse coding for each layer is used to extract features from time-series data. In addition, max-pooling is used to decrease the number of features for computation reduction (Boureau et al. 2010). The two layers method in Boureau et al. (2010) allows the local features and global features, respectively, to extract the learning system. The DL-based flow inference scheme has a higher positive rate and low false rate than ARMAX-least squares, Naïve Byes Classifiers, and Gaussian mixture models. In another work, Wang (2015) and Rehman et al. (2019), DL based traffic identification technique is proposed. In this method, the TCP flow is used for traffic identification, as the bytes of different protocol payloads represent different distributions. Thus, the bytes of TCP sessions are first normalized from integers to decimal, and then the normalized data is sent to ANN as the input for traffic identification. The authors proved that the scheme is more accurate than the state-of-the-art protocols. The DL based traffic classification technique was also used in Lotfollahi et al. (2017). The scheme is called "deep packet", which distinguishes traffic types, such as streaming and P2P, and classifies application types such as Spotify and Bit Torrent.

It is crucial for traffic identification to implement the DL algorithms on a specific layer. For instance, most of the traffic identification schemes are implemented upon transport layer, or IP layer (Wang 2015). However, some DL based schemes consider MAC layer or application layer features to identify the traffic type. For example, Gwon's scheme utilizes the runs-and-gaps model for the MAC layer as the input of the DL model and identifies the traffic type respectively (Gwon and Kung 2014). The work in Lotfollahi et al. (2017) also proposed traffic characterization and application identification to meet various requirements. However, the issue is to determine the features that can be used for DL analysis. The choice of data features used for DL models can significantly impact the accuracy of traffic identification.

3 Lesson learned

Based on the review of the literature on AI/ML approaches for security, we derive a set of key lessons learned to be considered in the implementation of AI/ML in security.

3.1 AI/ML approaches in future

AI and ML are sprinkling impact across every industry zone to produce novel competence and advantageous approaches for security purposes in data or an entire system. As AI and ML are working in tandem, AI influences ML abilities to improve intelligence and evolve the systems. Therefore, it will bring considerable benefit to identify the attacker and to protect against cutting-edge security intimidation. The InfoSecurity provider and facilitator, "Ryan Kh", pointed out that today's threats are more perplexing. It cannot be pinpointed by the existing obsolete security tools such as zero-day threats. Therefore, it poses a significant vulnerability to businesses and customers.

AI systems can control what is identified and recognized about the past attacks and threats to detect future attacks, in the same manner powered by ML algorithms. It is because attackers build older threats, using new abilities and modification by previously used samples. AI/ML is valuable to restrict the tide of zero-days threats by providing notification about emerging attacks. In the existing works, AI is normally used to distinguish simple threats and attacks. These simple attacks typically have simple solutions, which the system can easily handle the threat situations.

3.2 AI/ML to improve cybersecurity

From Sect. 3.2 (Machine Learning for Network/Cyber Security), we have learned that cybersecurity is one of the vital technologies to distinguish the most complex threats. Therefore, AI/ML can be regarded as a modern and promising defense against cybersecurity threats. In addition, the knowledge of understanding, representation, handling, AI/ML can significantly improve the cyber defense mechanisms by utilizing the latest algorithms. The exact controls and techniques should distinguish all the possible threats and defend against these attacks. Nevertheless, how can we preserve with the ever-evolving threat of a cyber-attack that is growing every year? Cybersecurity powered by AI can minimize the security threats and empower information technology teams to emphasize preventing the real threats. The ML algorithms can access the internal log of an organization while monitoring the systems to estimate users' patterns, activity profiles and keep the system protected around a clock (Li 2019).

AI will undoubtedly become irreplaceable once it identifies the threats in micro-deviations, indistinguishable from the human. Since AI tools are needed to feed more data over time, they can preserve a constantly moving standard. AI has no limitation in monitoring and evaluating the data compared to humans by the amount of data they can process in a day. However, the incomparable brainpower of an AI system gives it a unique benefit over humans when it comes to data processing and perceiving threats in cybersecurity. Conversely, most AI-based systems still struggle to implement suitable solutions once a security break is irreparable.

3.3 Future network security

AI is being applied more generally across industries, academia, and for a broad range of applications than ever before because of the increase in computing power, storage capabilities and data collection. This massive trove of data is a valuable forage for AI, which can process and analyze everything captured to comprehend novel developments and minutiae. However, hyper-connected workstations and the growth of cloud and mobile technologies have flickered a sequence of reactions regarding security risks. The gigantic volumes of associated devices serving into networks deliver a dreaming situation for cybercriminals. In addition, new and plentiful access points further face cyber-attacks and security on these access points is repeatedly lacking (Gopalsamy et al. 2020). According to a Cisco, report (Forecast 2016), the dramatic development of wireless devices will be more than 50 billion by the year 2030. Although this explosion of connected devices will make our daily lives and works easier, there are many risks. As per the report of PwC researchers (Yang et al. 2020), the number of global cyber-security events increased by 38%. It is also noted that security alerts flood the average enterprise from its cyber-security systems due to the increasing number of connected devices. Thus, AI/ML can overcome security alerts to revolve around processing and analyzing millions of data points at unbelievably high speeds.

The hackers also create malware attacks without breaking a system but remain within the victim's system for as long as possible (Zong et al. 2020). Another dangerous thing is that attackers can also use ML to fly under the radar of security systems by identifying and blocking cybercriminal activities. For example, researchers were capable of creating generative adversarial network (GAN) algorithms that make malware samples (He and Gan 2020; Thomas et al. 2020; Taheri et al. 2020). These malware samples can significantly sidestep ML-based security solutions intended explicitly to discover hazardous samples. Security specialists also predict that cybercriminals can employ ML to alter the code of new malware samples based on the security system that perceives previous infections. As a result, attackers can influence ML to construct more innovative malware detection that could potentially fly under the radar of security systems for a long time duration (Mizuno et al. 2017). This requires increasing the security posture and monitor the information technology. In addition, the researcher must ensure that users perceive the best fortification in their daily access and network activities. The attackers also utilize ML to gather all the information before they breach the target system (de Mello 2020). For instance, they collect the information of company stakeholders that would later be used to stimulate phishing attacks. The attackers also carry out research efforts with the help of ML and automatically increase the speed of the entire attack process. By leveraging ML, such kind of techniques exploits a spike in targeted attacks to utilize perceptible information. Therefore, it is quite essential to train and educate the researchers as part of a layered security posture to find out the proper solution to overcome the attacks.

3.4 Game theory or RL

All of the above works Chen et al. (2011, 2018a, b), Xiao et al. (2007, 2015, 2016a, b, 2017, 2018b, c), d), Tu et al. (2018c, 2020b, 2021), Feng et al. (2017b), Aljawarneh et al. (2018), Waqas et al. (2020b), Narudin et al. (2016), Han et al. (2016), Ahmed et al. (2018b), Zeng et al. (2018), Dai et al. (2019), Otoum et al. (2019), Conley and Miller (2013), Gwon et al.

(2013), Moore and Atkeson (1993), He et al. (2016), Amuru et al. (2016), Tello-Oquendo et al. (2018), Liu et al. (2013, 2014), Tugnait (2013), Jiang et al. (2013), Sutton and Barto (1998) and Amuru and Buehrer (2014) utilized the game theory and learning process of each player in the game. However, each player in practical security games usually has imperfect information about the adversary that provokes asymmetric information. In addition, stochastic game theory and multi-agent RL can offer a systematic structure to study the conflict-of-information. Thus, information asymmetry is needed to use the information unknown to the adversary for the player's benefit. For this purpose, minimax post-decision state and Win-or-learn fast post-decision state, the two multi-agent RL algorithms are designed in He et al. (2016) to enable the legitimate system to learn quickly by developing the information advantage in dynamic environments. These applications comprise (i) anti-jamming in energy harvesting communication systems, (ii) anti-jamming in cognitive radio and also (iii) cloud-based security games. In He et al. (2016), the jammer and the attacker cannot use the proposed algorithms due to information deficiency. However, there is a scenario where the attackers know the defenders' information and utilize the information to attain its learning states. In addition, none of the above works Chen et al. (2011, 2018a, b), Xiao et al. (2007, 2015, 2016a, b, 2017, 2018b, c), d), Tu et al. (2018c, 2020b, 2021), Feng et al. (2017b), Aljawarneh et al. (2018), Waqas et al. (2020a), Narudin et al. (2016), Han et al. (2016), Ahmed et al. (2018b), Zeng et al. (2018), Dai et al. (2019), Otoum et al. (2019), Conley and Miller (2013), Gwon et al. (2013), Moore and Atkeson (1993), He et al. (2016), Amuru et al. (2016), Tello-Oquendo et al. (2018), Liu et al. (2013, 2014), Tugnait (2013), Jiang et al. (2013), Sutton and Barto (1998) and Amuru and Buehrer (2014) considered the learning performance of physical layer jamming strategy where the jammer has incomplete or no information about the transmitter and the receiver.

3.5 Deep learning approaches

Security continues to be thoughtful a problem in any sector due to the increasing number of security breaks. It is believed that zero-day attacks are increasing day-by-day due to the addition of several protocols. Consequently, the ML approaches face difficulties for discovering these zero-day attacks (Wu and Guo 2020; Lobato et al. 2018). The DL approach is one of the practical approaches due to the improvement in the CPU performance. The utilization of DL is a strong mechanism to avoid zero-day attacks due to the high level of feature extraction ability. The key mechanisms of the DL architectures, such as self-taught and compression capabilities, are important features for unknown pattern detection (Li et al. 2018). Pattern detection can be distinguished from diverse traffic training data. The work done in Diro and Chilamkurti (2018) showed two analyses in terms of comparison between DL and other approaches as well as the distributed and centralized detection systems. It is found that the DL architecture is more efficient than the traditional ML approach for attack detection. The main reason is that the attack detection systems emphasize the detection speed rather than the learning speed. Consequently, the DL can alter the direction of attack detection in distributed environments. Therefore, the distributed attack detection systems are superior to centralized detection systems due to the DL architecture.

In a network, intrusion detection prevents the network from malicious attacks by identifying software interruptions. Although classical schemes are used for intrusion detection, these methods require administrative access to keep a considerable amount of user's signatures. Nowadays, anomaly-based detection is considered to examine network activities and point out data abnormality as an intrusion. The ultimate objective of intrusion detection

is to categorize the network traffic into two types, i.e., normal traffic and abnormal traffic. Thus, the DL approach is an appropriate choice to identify the network intrusions by acquiring traffic characteristics (Hodo et al. 2017).

3.6 Self-taught learning (STL)

The self-taught learning (STL) method is helpful to discover network intrusion (Javaid et al. 2016). However, the DL method in Javaid et al. (2016) chose 22 out of 41 features and had two stages for processing, i.e., an unsupervised feature learning based on sparse auto-encoder and a supervised learning procedure for classification. An auto-encoder is a feed-forward non-RNN protocol with input, output, and hidden layers. However, the input and output layers must be identical and more significant than the hidden layers. The DL network is also proposed for intrusion detection known as deep Boltzmann machine (DBM) (Tang et al. 2016), where nodes are connected among layers in both directions. However, RBM is used in Sun et al. (2018) to decrease the computation cost. Nevertheless, the network detectors do not understand the exact features of anomalous traffic in most real-time applications. Therefore, Fiore et al. (2013) suggested a discriminative RBM (DRBM) based intrusion detection scheme. This is a case of semi-supervised learning systems to train the data by using normal traffic data. The authors trained and tested the network using real-world traffic gathered from 24 h working stations and the KDD dataset. The datasets comprised both normal and abnormal data traffic. The outcomes showed that the learning system is trained and tested with high accuracy by about 94%. On the other hand, the accuracy is low for about 84% when DBRM is trained and tested with the KDD dataset. The DBM method can be transformed into a deep belief network (DBN) by limiting the node connection between layers.

3.7 Deep belief network (DBN)

The DBN is designed by cascading RBM and one or more layers to classify after a supervised learning procedure. As a result, DBM is mostly pre-trained by unlabeled data and then fine-tuned by labelled data, thus, achieving unsupervised and supervised learning, respectively. DBN is used for network intrusion detection where the learning network can be trained with KDD data in three phases (Mahfouz et al. 2020). In the first phase, the data is pre-processed for digitization and normalization. The second phase is to pre-train the DBN, i.e., the weights of RBMs stacks are learned through an unsupervised greedy contrastive divergence algorithm. The final stage is to weigh the entire DBN for a fine-tuned through the back-propagation errors using labelled data (Alom et al. 2015). The DBM method can also be used in the vehicle controller area network. In the controller area network, each packet consists of 12 bits of the arbitration field. Among these 12 bits, 6 bits are for the control field, and the rest of the bytes (data field) can be utilized for learning object (Kang and Kang 2016). This data field consists of mode information and value information. The mode information informs about the controlling wheel, and value information gives the information about the wheel angle of the electronic control unit. Due to different attack scenarios, the mode information is initially used to classify the attack scenarios. It can then train the learning network for various attack scenarios. The attack scenarios are determined by matching mode information in the testing phase to recognize the normal and abnormal packets (Tanveer et al. 2020).

3.8 ML and information theoretic security

Information-theoretic security (ITS) highly relies on fixed procedures to perceive the attacks based on known patterns. However, the approach has long ago reached its limitation. It is indicated that the time has come to consider the security arsenal for the current progress to the democratization of ML (Shakiba-Herfeh et al. 2020; Batra and Taneja 2020; Hartong and Roddy 2020). It incorporates an automatic data investigation to elevate the well-known indicator in the haystack that signifies an actual threat in the system. The attacks have become more complex in the last several years due to the expansion of infrastructure and applications. The utmost important aspect of analytics is the behaviour of the user. Therefore, understanding the users' behavior (normal or abnormal) is a serious component of discovering threats. Nevertheless, to encourage users' behavior analytics, we should know who the users are. In this regard, the identity and access management (IAM) systems can provide an identity context with attributes, such as role, titles, and organizational structure to improve and control the information and risks. For instance, risk-based authentication (RBA) shows diverse parameters (i.e., location, device, IP address and history, access information and specific user attributes) to control the risks. In this regard, particular requirements are needed. In addition, adaptive certification is also an example of the risk data usage in IAM. However, the risks are also based on static instructions, and ML can offer more opportunities to measure these risks dynamically.

Nowadays, our daily use appliances and vehicles are becoming Internet-enabled. However, Internet-enabled devices are more vulnerable to security threats in our organizations. Hackers can easily take advantage of insufficient protection because these devices are directly linked to the network. Thus, the attackers could laterally move within the network to breach the critical information and systems. Due to the thousands of wireless devices and their corresponding data, we would be overwhelmed by manually managing and tracking all devices and data. Nevertheless, we can leverage ML technology to investigate the data and network connections. In this way, it becomes easier to recognize abnormal activity and block destructive activities. ML-based systems are proficient at exploring via extensive data set and modifying themselves based on specific trends. The security solution can easily be incorporated with ML to identify network changes over time and modify the behavior of users' profiles.

4 Open problems

The integration of AI in security has been broadly studied to solve different technical problems in the past few decades. However, there are some special concerns for security owing to new requirements and use cases. Consequently, we list the open issues that deserve further investigation.

4.1 Standardization

Numerous frameworks, algorithms and optimization techniques have been suggested for security. However, the research efforts towards security by exploiting ML techniques are still in their infancy. There are diverse attacks that impend ML techniques for security purposes, as the statistical ML greatly relies on data quality. The data might be feeble to

protect against the adversarial samples. The data collection and predication of adversarial samples is a challenging task in the implementation of ML-based detection procedures for pinpointing malicious data. Therefore, there is a need to design new adversary models under the perception of attackers. Essentially, we need to pay more attention to analyze security in the decision systems due to the abrupt increase of security threats. Thus, standardizing the former security methods to novel ML techniques is still in the early phase. It is essential to implement and well-defined security standards in future.

Despite a significant advancement of different proposals to ensure the security of users, it is suffering from the low-cost productivity due to multifaceted cryptographic processes on ML algorithms (Pihur and Korolova 2014). Hence, it is highly recommended to investigate the efficient more efficient techniques in an adversarial environment. Existing research also verifies that the counterintuitive features of DNNs affect security. Irrespective of suggestions on adversarial data in training models and enlightening the strength of ML algorithms, these solutions are still feeble to discourse the problems mentioned above. Thus, secure DL models is a very stimulating research direction such as Bayes deep networks (Wang and Yeung 2016). Commonly, a high degree of security encourages a higher overhead or even a lower performance of learning algorithms. Hence, the designing of proper ML algorithms is suggested to assist in practical scenarios.

4.2 Integration of machine learning techniques

It is essential to overcome the problem of how to integrate ML techniques, such as ANN, DL and RL, into future wireless communication (Sagduyu et al. 2020). This is because the integration of ML techniques into wireless communication may affect the transmission technologies as well as considerably influence how the networks need to be measured via feedback signals to circumvent insatiability as well as malfunctioning (Tomasin 2018; Tu et al. 2018a, b). We find out that DL and RL can be implemented in a distributed manner. Nevertheless, several problems need to be solved in the coming years. For instance, users having their own ANN in a distributed network must be trained based on a dataset obtained from experience and dataset measurements. It certainly indicates a distinctive node that has diverse learning abilities. Also, each distributed dataset is different in size because other users have separate measurement and storage capabilities. Since each user will experience different data because of various measures, this leads to instability and can crash the wireless communication. Another subject to address is the possibility of each user optimizing its performance in a distributed setup rather than system utility. This will cause a device to learn how to cheat for specific gain. Therefore, security techniques should be considered carefully to guarantee wireless communication in a precise way (Rath and Mishra 2020).

Another task is to solve the problem of robustness in DL against corrupted information. For instance, the datasets utilized for training/learning purposes might be corrupted and possibly lead to unfavorable outcomes. This is due to an inevitable error over the feedback channels and data storage procedure. ML techniques must practically exploit the training process, mainly from the distributed implementation of ANN-based wireless networks. This will cause prone the entire network to inconsistencies and disasters. Furthermore, a future research direction to get a cross-fertilization between mathematical models and DL is to derive a theoretical analysis of how ANN works and configure specific tasks. The problem of the black box in ANNs is to understand and regulate the behavior of users is another important matter for future research.

4.3 Cyber-infrastructure

The threats to the cyber-infrastructure are growing dramatically. For the last couple of years, security breaches are rising exponentially. Poor security techniques are promoted into global phenomena. Nevertheless, the growing incidents of malware and ransomware attacks are tackled with comprehensive awareness and preventive steps for the ever-growing complex levels of attackers. For instance, the current scenario of spams is worse than as these spams attack is for the short duration of time (Ahuja et al. 2020; Belciug and Gorunescu 2020). Indeed, some of the spam is tackled down, but most of the spam can attack by the ignorance of users and is vulnerable by clicking on malicious links. Consequently, it can be triggered by a ransomware or password break. One of the recent technologies, i.e., Blockchain, can be exploited to tackle security breaches. Blockchain can be used as a security technology that takes attention for future directions. It can eradicate the use of passwords, providing innovative encryption procedures. Consequently, blockchain security will unquestionably be an intriguing arena in the future cyber-security.

In the last couple of years, we notice highly publicized ransomware attacks. Usually, the attackers acquire their pay-out, and most indemnities occur in reputation, legal costs, and the confidence level of an organization (Patel and Tailor 2020). However, even the inexperienced attackers can quickly introduce a ransomware attack through RaaS (Ransomware as a Service) (Sharmeen et al. 2020; Butt et al. 2020). Ransomware, along with phishing attacks, has been one of the major concerns in recent years. In this case, we need to notice the impact of cryptocurrency valuation by utilizing AI/ML.

4.4 Social engineering

Another area for future recommendation is the use of AI/ML in social engineering. The reason is that social engineering is growing in the field of wireless networks, and correspondingly the cyber-crime increases. For example, one of the industrial reports shows that phishing attacks increased by almost 74% in 2017 and will surge in the future (Ozcelik 2020; Zheng et al. 2020). It is mainly attributed to human error and can be removed with the help of AI/ML. In an ideal scenario, we can be skilled to predict these phishing attacks in advance and tackle these kinds of problems in future. As we talked about industry reports, there is also an increased concentration of scammers targeting the attacks based on large pay-out known as industry-specific attacks: these pay-outs access financial transactions and data value. The healthcare sector also has valuable information and will endure seeing a surge in attacks. However, the arena is shifted to more pay-off based scams. With the proliferation of "Bring Your Device", scammers have recognized that it is treasured to approach the entire network than individual users (Ameen et al. 2020; Singar and Akhilesh 2020; Geogen and Poovammal 2020). Likewise, as everything is shifted towards the cloud and the standard and traditional firewall ideas are changing, researchers are seeking new techniques to secure the networks, i.e., email archiving, encryption, URL defense, and so on. Thus, companies continuously intensify their attention on robust processes and training as a significant preventive measure due to the continuous progress in diversity, i.e., how and where the employees access the networks.

4.5 Access control

The access control means that every user should approach the network. Hence, the access control pursues to prevent illegal activities that lead to the security breach. To defend from possible attacks, we need to identify every user and device. For this purpose, we need some security policies to access the entire network. For instance, we can block non-compliant devices or provide them with limited access. The procedure is called network access control which is delivered using different methods to control network access by the authentic users. It also offers a defined security policy maintained by a network access server to provide essential access towards authentication and authorization. Access control is vital for secrecy, integrity, and accessibility purposes.

The threats are increasing continuously as more and more people continue to use networks. IoT comes with innovative development, and it can be noticed that over 70% of the IoT devices are vulnerable to security threats by opening up unlimited chances for hackers, and scammers (Bernal 2020; Chernov and Sornette 2020). The reason is that uncertain web interface, and data transfer will make the users susceptible to attacks. Another reason is that multiple devices are connected. Hence, all devices can be easily accessible if one device is breached. In short, we can say that cybercriminals increase the number of jobs in cybersecurity. Nevertheless, the battle appears to be incessant and will not come to an end. Therefore, AI will take over some of the encumbrances in cybersecurity.

5 Conclusion

This work furnishes a detailed survey of the state-of-the-art in security and the impact of AI on security. We have reviewed a broad spectrum of research on the subject and have foregrounded the significant findings. We have carved up the survey into three significant sections. The first part categorizes security branches and threats that are essential to be tackled in future. We illustrate both communication security and network security and deliver a complete and hierarchical taxonomy of security threats from both perspectives, i.e., communication and network security. After an insightful view of the security threats, we categorize and explain distinct aspects of AI that can solve the security threats. Therefore, the second part of the paper deals with technical problems and proposed solutions for security through AI. Although security threats are well investigated in different attractive directions, yet we focus on the security attacks that ML solves for communication and network security. In the third part, we illustrate the lessons learned from the existing techniques and contribution of up-to-date literature. In addition, we distinguish open problems that merit future research directions. We believe that the discussion presented in this review will suffice as a reference guide for researchers and developers to facilitate the design and implementation of AI in security.

Appendix 1: Recent attacks

There are several attacks on different applications and organizations in recent years. Some recent attacks are discussed as follows.

1. In 2019, Instagram discovered that an unsecured server containing the personal information of millions of Instagram influencers, celebrities, and brand accounts had been found online (Fatma et al. 2020). The details revealed the biodata of users, profile photos, followers information, location, nation, and contact information (Jonathan and Oeldorf-Hirsch 2020).
2. On 30 August 2019, I.T. managers in the headquarters of the United Nations in Geneva alerted their security departments of an instance of hacking. The authorities pointed out that the complex cyberattack on U.N. in Geneva and Vienna had started more than a month earlier (Caravelli and Jones 2019; Keetharuth et al. 2019).
3. In 2019, one of the most significant breaches of *"corporate data"* was on the American medical collection agency, a massive debt collector in the field of healthcare (Connor 2019). The company found that the breach occurred in March, and a report to the U.S. Securities and exchange commission revealed that the breach into infrastructure lasted for almost eight months. The event was first publicly reported in early June 2019, and 7.7 million users had data exposed (Steward and Cavazos 2019).
4. According to BBC News, Travelex's U.K. international money transfer service and wire crippled by a ransomware attack (Valdeón 2019; Emami et al. 2019). The attacker forced the staff to use paper and pen to calculate currency exchanges. The cyberattack prompted the company to take off all its devices and caused chaos among new year holidaymakers and business travellers searching for electronic monetary services.
5. Canva is the online design tool in Australia. In May 2019, Canva revealed that hackers break their network and steal the data of about 140 million users (Head 2019). They stole information contains the users' usernames and email addresses. Fortunately, the hackers were unable to steal the users' credit card details (Natalya 2019).
6. DoorDash is a food delivery service provider in San Francisco. DoorDash faced a huge data breach by affecting the data of 4.9 million users on May 4, 2019 (Bill et al. 2019).
7. On 28 Feb. 2018, GitHub was hit with a massive denial of service attack with a data rate of 1.35 TB/s (Gupta and Sharma 2018). Even if GitHub was intermittently knocked offline and managed to overthrow the attack after less than 20 minutes, the scale of the attack was devastating.
8. WannaCry was a rapidly spreading ransomware attack in May 2017 (Patel and Tailor 2020). Like all ransomware, it took over malicious software, encrypted their hard drive files, and then requested payment in Bitcoin for decryption (Prasad and Rohokale 2020). The malware has taken a particular root in computers at facilities operated by the U.K.
9. The massive breach into Yahoo's email system receives an honorable mention because it happened way back in 2013—but the extent of it, involving almost 3 billion Yahoo email addresses, only became evident in October 2017 (Srinivas et al. 2020). Stolen information contained credentials and email addresses for protection, secured using old, easy-to-crack methods used by software criminals to hack other accounts (Siponen et al. 2020).
10. In 2017, Equifax Inc. declared that there was a cyber-security breach between May and mid-July of the same year (Lohstroh 2017). As a result, about 145.5 million U.S. cybercriminals had reached personal data of Equifax customers, including their full names, social security numbers, credit card details, dates of birth, residences and, in some cases, the numbing of the driver's license (Diesch et al. 2020).

Appendix 2: Security branches

1. *Communication security* Communication security requires that physical as well as digital data must be secured or protected from any non-legitimate users, access, revelation, disturbance, alteration, inspection, recording, or demolition (Liu et al. 2020a; Waqas et al. 2018d). Communication security is different from other security in the sense that it keeps the data secure. For instance, it targets to keep the transmitted information protected while cyber-security fortifies only digital information. Therefore, the professionals in communication security acquire diverse strategies and practices for an actual information security paradigm (Haus et al. 2017), which is referred to as the CIA (confidentiality, integrity and availability) triad.
2. *Network security*

   Network security lies in the network layer to keep the network, and its reliability against hacking as well as unauthorized access (Chen et al. 2020; Ahmed et al. 2018a). It is aimed at preventing data transfer among devices in the network. Consequently, it makes sure the data is not altered/changed or interrupted. It is necessary for the security team to essentially implement the software and hardware to defend the system/organization's infrastructure. Furthermore, network security detects the embryonic risks before the attackers penetrate the system and steal/destroy the users' data. Moreover, the job of network security management is to ensure that the network is more secure by delivering technical expertise. The priority for the network security management is to get the attackers out as quickly as possible if the network security is compromised. This is necessary because as long as the attackers stay in the network, they can steal more data in more time available for them. Therefore, to alleviate the total cost, the best solution is to hastily recognize, stop and extrude the attacker from the network.
3. *Cybersecurity*

   Cybersecurity is the practice to defend any organizations' network, workstations and information from any illegitimate digital access, attacks/impairment by imposing diverse procedures, engineering and practices. It is essential to secure the information technology infrastructure of any organization all the time from the prevention of full-scale attacks and hazards that expose the organization data, and repute (Kharraz et al. 2018). Cybersecurity protects the integrity of the networks from unauthorized electronic access by implementing various security measures and controls (Zhang et al. 2021). The threat players manipulate the users to give access to their sensitive data.
4. *Difference between cyber and network security*

   It is believed that the Internet has revolutionized everything by changing how we do things. Companies like Amazon, eBay, Ali Baba, JingDong, Google, Facebook and Twitter have made everything easily accessible at their fingertips. Our daily routine business becomes more digitally advanced, and as technology progress, the security infrastructure must be appropriately stiffened. Cybersecurity is a technique to keep interconnected systems/networks secure from digital attacks (Smith 2020). Cybersecurity assists the system/network from the external extortions. It defends the systems and programs from all sorts of digital attacks like phishing and baiting. On the other hand, network security exploits files and directories in the network against maltreatment and illegal access. Thus, network security is to defend the information technology of the organization from online threats.

Appendix 3: Security threats

We have amalgamated diverse types of security threats in this work. These attacks are interlinked and can attack communication security and attack in network and cyber warfare. These security threats are discussed point by point as follows.

1. *Rogue wireless devices*
   Rogue wireless devices might be access points or end-users that can pose security threats towards the wireless networks (Zaidi et al. 2016). These devices can reveal confidential information and is possibly damaging the wireless networks. The rogue devices intrude in the wireless communication, deprived of authentication and authorization to become the wireless access points. These rogue wireless access points can gather users' private data (Lu et al. 2018b; Xiao et al. 2019) without the permission of the network administrator and avoid security policies. In addition, rogue devices can also permit other unauthorized users to become a part of the communication system and utilize the resources (Zhou et al. 2017b).
2. *Eavesdropping*
   In wireless communication, an eavesdropping attack is an incursion where unauthorized/non-legitimate users try to steal the information between two authorized/legitimate users, as depicted in Fig. 5. An eavesdropping attack is difficult to detect since it would not cause communications to be operated abnormally but trying to listen to the communication silently (Waqas et al. 2018a). Eavesdropping is an unauthorized digital communication, real-time interruption of private communication, for instance, audio and video calls, text or fax messages. Eavesdropping not only occurs in communication but is also a challenge in network security and cybersecurity. Network eavesdropping emphasizes capturing (without altering) small packets transmitted in the network to get valuable information. On the other hand, cyber attackers can record sensitive information by sniffing the insecure networks. The packets in networks are usually encrypted. However, they can be viewed by utilizing cryptographic tools.
3. *Man-in-the-middle attacks (MITM)*
   In a MITM attack, an unauthorized user jumps into the communication between authorized users and imitates both parties by pretending to be an authentic user, as shown in Fig. 6. In this way, MITM can gain access to information that the two authentic users are trying to communicate. However, MITM also permits malicious users to interrupt and transmit/receive data intended for authorized users. This attack is similar

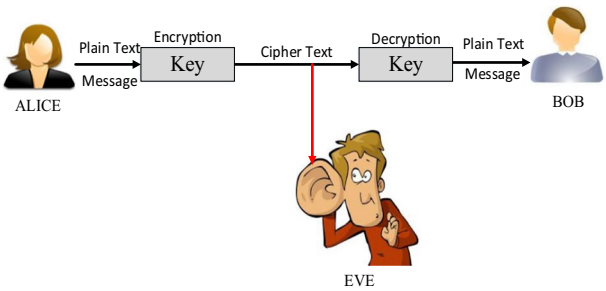

Fig. 5 Eavesdropping attack

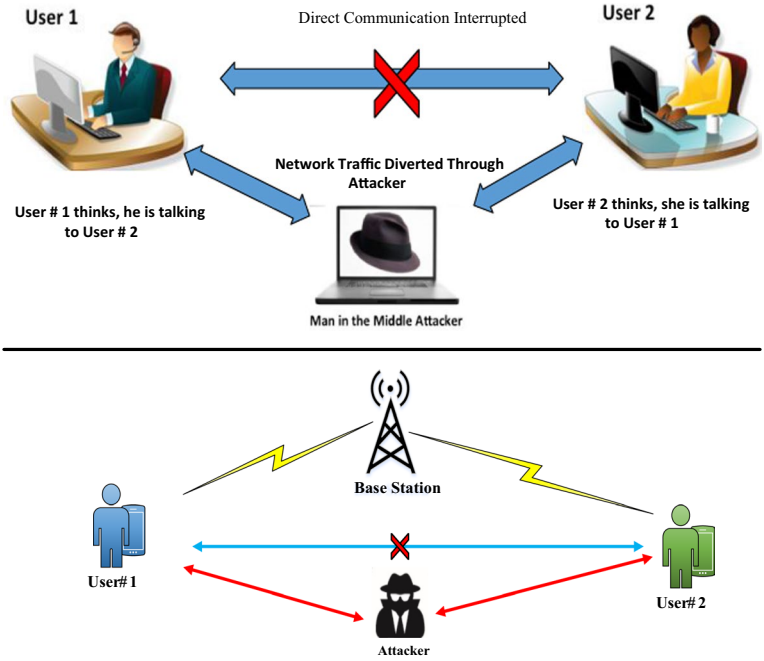

Fig. 6 Man-in-the-middle attack

to the eavesdropping attack. However, eavesdropper only listens to the communication between the authentic users. On the other side, MITM can listen to the communication, but it imitates the authentic users and can alter the information of the authentic users.

4. *Data integrity attacks*

   Data integrity attacks compromise the reliability of transmitted data over wireless communication links. The data integrity attack is observed as message modification and jamming attacks in wireless networks. In the message modification, the attack is based on the addition or deletions of the actual data by adversaries. On the other hand, a jamming attack disrupts the communication link by transmitting jamming signals. It limits the signal to interference noise ratio (SINR) of the communication link and can also result in partial disruptions. The data integrity attacks are also linked with authentication-based attacks. The authentication attacks can lead to the data integrity problems, such as altering the data. Therefore, integrity checks, i.e., key-based techniques or pre-determined packets, are necessary to detect integrity attacks.

5. *Robustness attack*

   The primary robustness attacks are DoS, and disruptive denial of service (DDoS) (Yuan et al. 2018). A DoS targets the network resources to disrupt communication among the authentic users. In addition, DDoS attacks endeavour to devastate resources, such as websites, game servers, and DNS servers, with traffic flooding as illustrate in Fig. 7. Typically, the goal of DDoS is to slow down or destroy the system. The countermeasures of DoS and DDoS attacks are not clear, as these attacks can be implemented in different ways. Moreover, the inconsistency detection systems are a countermeasure if an attack is being held for any network resources. To preclude a detected DoS/DDoS attack, the resource procedure of the adversaries is blocked, or a

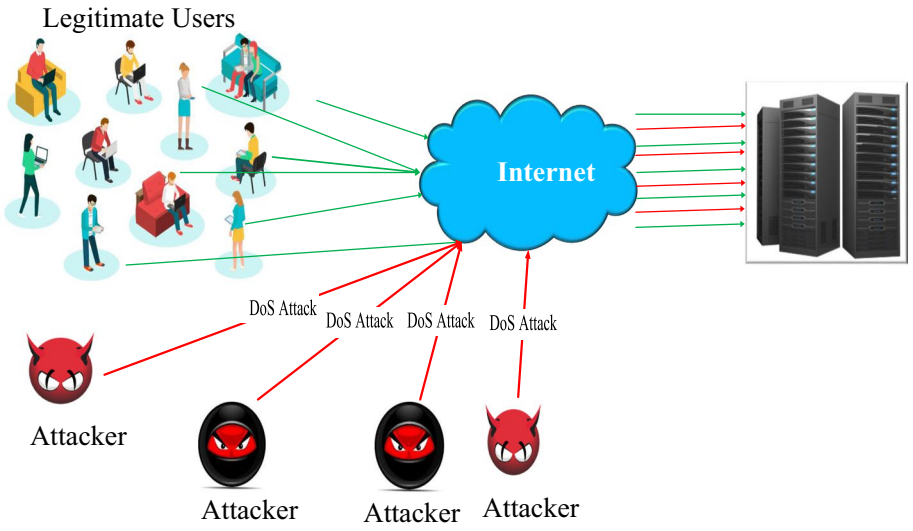

Fig. 7 Denial-of-Service attack

backup resource is used. For example, a network controller node generally precludes the attackers by blocking their resource usages if the DoS/DDoS is detected in the network. Another technique is to differentiate the network resources by using backup resources to increase the vitality of the communication system.

6. *Malware attack*

   A malware attack includes viruses, worms, spyware, trojans, and ransomware. Malware is a malicious software application to harm or hijack the network (Liu et al. 2020b). It is an extensive and well-known attack that includes the following three common ways.

   (a) Phishing e-mails: The attackers can generate an e-mail to entice the authentic users into a false sense of reassurance. The attackers also trick the target users into downloading the attached files that would be malware.
   (b) Malicious websites: The attackers can create websites that manipulate the kits designed to discover vulnerabilities in the system. It may motivate the victim to use those websites and automatically install malware onto their systems.
   (c) Malvertising: Some cunning attackers reveal different techniques to use the advertising to distribute their wares. By clicking the advertisement, the malicious adverts will redirect the users to malware-hosting websites.

7. *Data loss/leakage*

   Data leakage is an illegal data communication from network to peripheral recipient (Lu et al. 2018a). Alternatively, data loss is any activity that corrupts the data, erases the data or makes it unreadable to users, software or application (Huang et al. 2018). The threat usually occurs via the web and e-mail. However, it also happens via mobile data storage devices such as optical medium, USB, and PCs. Data exploitation, deliberation, and stealing are why data loss/leakage may occur. Therefore, defensive mechanisms are necessarily required to guarantee the prevention of common data leak-

age threats. In this regard, a data loss prevention (DLP) strategy is adopted to make it inevitable that authentic users do not convey their sensitive data outside the network.

8. *Brute force attack*

In a brute force attack, the cryptanalyst will attempt to decrypt any encrypted data as shown in Fig. 8 (Ricci et al. 2019). The attacker attempts all conceivable passwords and pass-phrases until the attacker gets corrected one. Thus, the attacker can struggle to estimate the key predictably generated from the password utilizing the key derivation function, known as exhaustive key search. The attacker tries to discover the system or service's password via trial and error rather than trick a user into downloading the malware.

9. *Smurf attack*

In a smurf attack, the network is deluged by fake messages. The Smurf attacks take specific distinguishing facts into consideration about the ICMP. In ICMP, the network administrators are responsible for exchanging the network state information and ping other nodes to control their operating status. A smurf attack transmits the spoofed network packets Anjomshoa et al. (2017) that include an ICMP ping as depicted in Fig. 9. As a result, the number of pings and subsequent echoes make the network unstable and not usable for real traffic. To avert a Smurf attack, the hosts and routers must be designed to not respond to external ping requests in the networks. The routers should configure to assure that the data are not forwarded to those external ping requests.

10. *Spoofing attack*

Spoofing is an attack that involves malicious users by impersonating the authentic device/users. The spoofer can introduce an impersonation attack in the network while stealing information and spread malware or bypass the access controls, as depicted in Fig. 10. Spoofing attacks can be distinguished into several common attacks, such as IP spoofing, address resolution protocol, e-mail and DNS server spoofing attacks. Spoofing attacks are also an extensive dilemma in wireless networks because they do not draw the same level of attention as other attacks. In many cases, this is worsened as

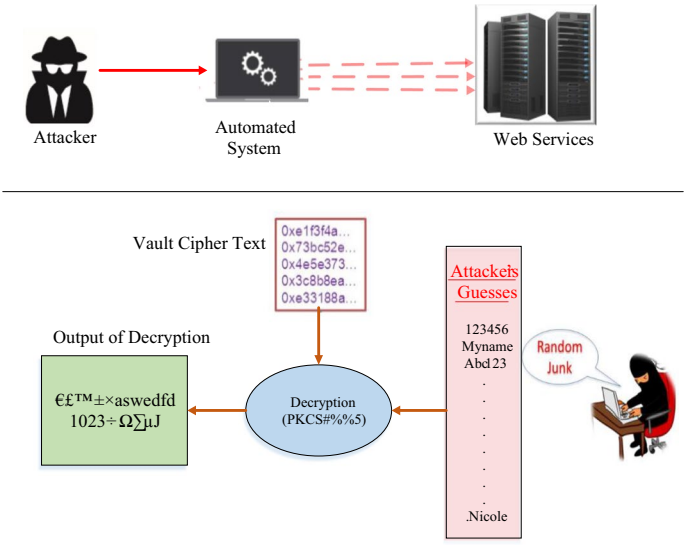

Fig. 8 Brute force attack

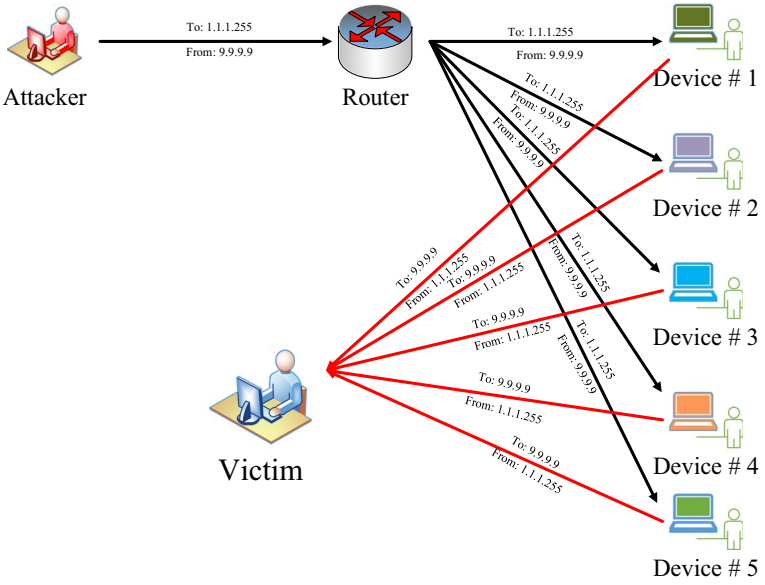

Fig. 9 Smurf attack

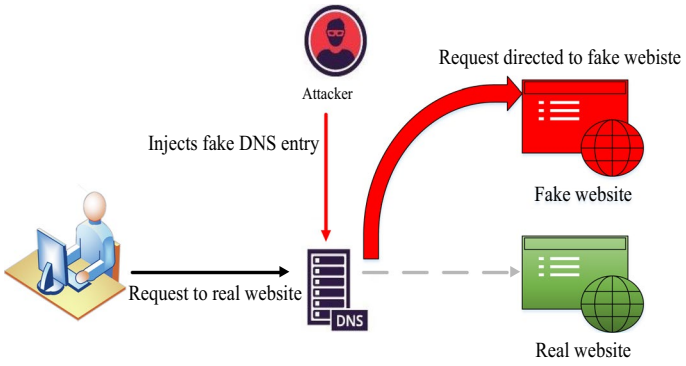

Fig. 10 Spoofing attack

the user is not safe from spoofing attacks without the proper training and equipment. A relatively skilled attacker can avoid the defense and access the correct data. Therefore, the awareness of the spoofing attacks and implementing measures to protect against diverse types of spoofing attacks are the only ways to protect the network.

11. *Hijacking* Hijacking uses IP addresses to transmit the data over the Internet. It is a less known cyberattack that may have devastating consequences on the networks, such as financial institutions, commercial and government services. IP hacking manipulates some weaknesses in general IP networking and the border gateway protocol, which defines paths for transmitted data packets. IP hijacking can be used for several kinds of targeted activities, such as spamming, DoS, DDoS, malware and record-breaking data

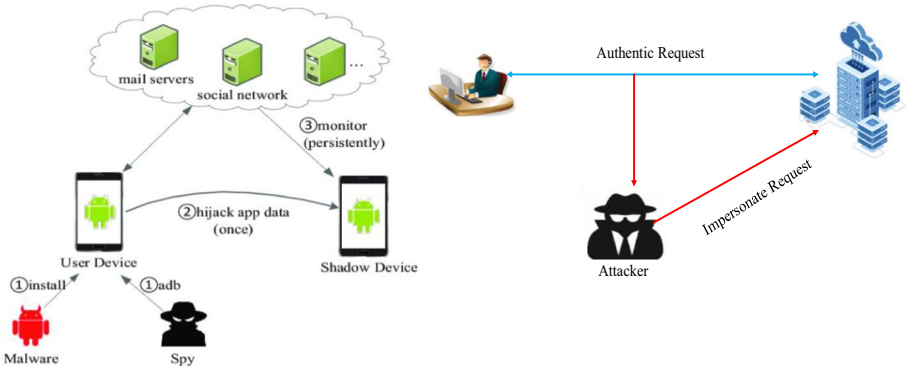

Fig. 11 Hijacking **a** data hijacking, **b** session hijacking

breaches attacks. These attacks are considered the most significant attack in history due to IP hijacking. Figure 11 shows two types of hijacking attacks, i.e., (a) shows the data hijacking while (b) illustrates the session hijacking.

References

Ahmed M, Shi H, Chen X, Li Y, Waqas M, Jin D (2018a) Socially aware secrecy-ensured resource allocation in D2D underlay communication: an overlapping coalitional game scheme. IEEE Trans Wirel Commun 17(6):4118–4133

Ahmed M, Li Y, Waqas M, Sheraz M, Jin D, Han Z (2018b) A survey on socially aware device-to-device communications. IEEE Commun Surv Tutor 20(3):2169–2197

Ahuja R, Chug A, Gupta S, Ahuja P, Kohli S (2020) Classification and clustering algorithms of machine learning with their applications. In: Yang X-S, He X-S (eds) Nature-inspired computation in data mining and machine learning. Springer, pp 225–248

Alauthaman M, Aslam N, Zhang L, Alasem R, Hossain MA (2018) A P2P botnet detection scheme based on decision tree and adaptive multilayer neural networks. Neural Comput Appl 29(11):991–1004

Aljawarneh S, Aldwairi M, Yassein MB (2018) Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. J Comput Sci 25:152–160

Alom MZ, Bontupalli V, Taha TM (2015) Intrusion detection using deep belief networks. In: National aerospace and electronics conference (NAECON), pp 339–344

Ambekar A, Schotten HD (2014) Enhancing channel reciprocity for effective key management in wireless ad-hoc networks. In: IEEE 79th vehicular technology conference (VTC Spring), pp 1–5

Ameen N, Tarhini A, Shah MH, Madichie NO (2020) Employees' behavioural intention to smartphone security: a gender-based. Cross-national study. Comput Hum Behav 104:106184

Amuru S, Tekin C, v der Schaar M, Buehrer RM (2016) Jamming bandits: a novel learning method for optimal jamming. IEEE Trans Wirel Commun 15(4):2792–2808

Amuru S, Buehrer RM (2014) Optimal jamming strategies in digital communications impact of modulation. In: IEEE global communications conference, pp 1619–1624

Prasad R, Rohokale V (2020) Malware. In: Cyber security: the lifeline of information and communication technology. Springer, Berlin, pp 67–81

Anjomshoa F, Kantarci B, Erol-Kantarci M, Schuckers S (2017) Detection of spoofed identities on smartphones via sociability metrics. In: IEEE international conference on communications (ICC), pp 1–6

Ayodeji O et al (2021) Security and privacy for artificial intelligence: opportunities and challenges. arXiv:2102.04661

Batra L, Taneja H (2020) Evaluating volatile stock markets using information theoretic measures. Phys A Stat Mech Appl 537:122711

Belciug S, Gorunescu F (2020) Era of intelligent systems in healthcare. In: Dorgham MA (ed) Intelligent decision support systems-a journey to smarter healthcare. Springer, Berlin, pp 1–55
Bellet A, Liang Y, Garakani AB, Balcan MF, Sha F (2015) A distributed Frank–Wolfe algorithm for communication efficient sparse learning. In: Proceedings of the 2015 SIAM international conference on data mining, pp 478–486
Bernal P (2020) What do we know and what should we do about internet privacy? SAGE Publications Limited, Thousand Oaks
Bhuyan MH, Bhattacharyya DK, Kalita JK (2013) Network anomaly detection: methods, systems and tools. IEEE Commun Surv Tutor 16(1):303–336
Bill L, Curtis W, Bedford D, Iyer S (2019) The knowledge economy: implications for organizations. Work and workers, knowledge economies and knowledge work (Working methods for knowledge management), pp 41–64
Blatt D, Hero AO, Gauchman H (2007) A convergent incremental gradient method with a constant step size. SIAM J Optim 18(1):29–51
Boureau Y-L, Ponce J, LeCun Y (2010) A theoretical analysis of feature pooling in visual recognition. In: Proceedings of the 27th international conference on machine learning, pp 111–118
Buczak AL, Guven E (2016) A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Commu Surv Tutor 18(2):1153–1176
Butt UJ, Abbod MF, Kumar A (2020) Cyber threat ransomware and marketing to networked consumers. In: Dadwal SS (ed) Handbook of research on innovations in technology and marketing for the connected consumer. IGI Global, pp 155–185
Caravelli J, Jones N (2019) Cyber crime. In: Paige D (ed) Cyber security: threats and responses for government and business. ABC-CLIO, pp 23–43
Chatterjee B, Das D, Maity S, Sen S (2019) RF-PUF: enhancing IoT security through authentication of wireless nodes using in-situ machine learning. IEEE Internet Things J 6(1):388–398
Chen J, Yu Q, Cheng P, Sun Y, Fan Y, Shen X (2011) Game theoretical approach for channel allocation in wireless sensor and actuator networks. IEEE Trans Autom Control 56(10):2332–2344
Chen Y, Zhang Y, Maharjan S (2017) Deep learning for secure mobile edge computing. CoRR arxiv: abs/1709.08025
Chen G, Zhan Y, Chen Y, Xiao L, Wang Y, An N (2018a) Reinforcement learning based power control for in-body sensors in WBANS against jamming. IEEE Access 6:37403–37412
Chen Y, Poskitt CM, Sun J (2018b) Learning from mutants: using code mutation to learn and monitor invariants of a cyber-physical system. In: IEEE symposium on security and privacy, pp 648–660
Chen L, Yi Z, Chen X (2020) Research on network security technology based on artificial intelligence. In: Kacprzyk J (ed) Recent trends in intelligent computing, communication and devices. Springer, Berlin, pp 729–735
Chernov D, Sornette D (2020) Specific features of risk management in the industrial and agricultural sectors. In: Critical risks of different economic sectors. Springer, Berlin, pp 13–145
Conley WG, Miller AJ (2013) Cognitive jamming game for dynamically countering ad-hoc cognitive radio networks. In: MILCOM 2013—2013 IEEE military communications conference, pp 1176–1182
Connor OP (2019) 2019 security lockdown or hacker bonanza. ITNOW 61(4):44–45
Dai HN et al (2019) Big data analytics for large-scale wireless networks: challenges and opportunities. ACM Comput Surv (CSUR) 52(5):1–36
de Mello FL (2020) A survey on machine learning adversarial attacks. J Inf Secur Cryptogr (Enigma) 7(1):1–7
Dibaei M et al (2020) Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: a survey. IEEE Trans Intell Transp Syst. https://doi.org/10.1109/TITS.2020.3019101
Diesch R, Pfaff M, Krcmar H (2020) A comprehensive model of information security factors for decision-makers. Comput Secur 92:101747
Diro AA, Chilamkurti N (2018) Distributed attack detection scheme using deep learning approach for Internet of Things. Future Gener Comput Syst 82:761–768
Draper-Gil G, Lashkari AH, Mamun MSI, Ghorbani AA (2016) Characterization of encrypted and VPN traffic using time-related. In: Proceedings of the 2nd international conference on information systems security and privacy (ICISSP), pp 407–414
Emami C, Smith RG, Jorna P (2019) Predicting online fraud victimisation in Australia. Trends Issues Crime Crim Justice no 577, p 1
Eslahi M, Yousefi M, Var Naseri M, Yussof YM, Tahir N, Hashim H (2016) Mobile botnet detection model based on retrospective pattern recognition. Int J Secur Appl 10:39–44

Fatma S et al (2020) Modelling perceived risks to personal privacy from location disclosure on online social networks. Int J Geogr Inf Sci 34(1):150–176
Feng Q, Dou Z, Li C, Si G (2017a) Anomaly detection of spectrum in wireless communication via deep autoencoder. In: Advances in computer science and ubiquitous computing, pp 259–265
Feng C, Wu S, Liu N (2017b) A user-centric machine learning framework for cybersecurity operations center. In: IEEE international conference on intelligence and security informatics (ISI), pp 173–175
Fiore U, Palmieri F, Castiglione A, De Santis A (2013) Network anomaly detection with the restricted Boltzmann machine. Neurocomputing 122:13–23
Forecast CGMDT (2016) Update Report, 2014–2019, Cisco white paper
Geogen G, Poovammal E (2020) Mobile malware, securing the internet of things: concepts, methodologies, tools, and applications. IGI Global, Hershey, pp 92–108
Gopalsamy BN, Brindha G, Santhi B (2020) Implementation of machine learning in network security. In: Solanki A, Kumar S, Nayyar A (eds) Handbook of research on emerging trends and applications of machine learning. IGI Global, pp 276–299
Gu X, Li X (2016) A detection method for network security based on the combination of support vector machine. In: Third international conference on artificial intelligence and pattern recognition (AIPR), pp 1–5
Gupta V, Sharma E (2018) Mitigating DNS amplification attacks using a set of geographically distributed SDN routers. In: IEEE international conference on advances in computing, communications and informatics (ICACCI), pp 392–400
Gurbuzbalaban M, Ozdaglar A, Parrilo PA (2017) On the convergence rate of incremental aggregated gradient algorithms. SIAM J Optim 27(2):1035–1048
Gwon YL, Kung H (2014) Inferring origin flow patterns in wi-fi with deep learning. In: 11th international conference on autonomic computing, pp 73–83
Gwon Y, Dastangoo S, Fossa C, Kung H (2013) Competing mobile network game: embracing anti-jamming and jamming strategies with reinforcement learning. In: IEEE conference on communications and network security (CNS), pp 28–36
Hajoary PK, Akhilesh K (2020) Role of government in tackling cybersecurity threat. In: Akhilesh KB, Möller DPF (eds) Smart technologies. Springer, pp 79–96
Hamedani K, Liu L, Atat R, Wu J, Yi Y (2018) Reservoir computing meets smart grids: attack detection using delayed feedback networks. IEEE Trans Ind Inf 14(2):734–743
Han Y, Alpcan T, Chan J, Leckie C, Rubinstein BI (2016) A game theoretical approach to defend against co-resident attacks in cloud computing: preventing co-residence using semi-supervised learning. IEEE Trans Inf Forensics Secur 11(3):556–570
Hartong MW, Roddy SA (2020) An information theoretic approach to platform technology selection to aid influence operations. IEEE Syst J 14(4):5308–5319
Haus M, Waqas M, Ding AY, Li Y, Tarkoma S, Ott J (2017) Security and privacy in device-to-device (D2D) communication: a review. IEEE Commun Surv Tutor 19(2):1054–1079
He P, Gan G (2020) Android malicious APP detection based on CNN deep learning algorithm. In: IOP conference series: earth and environmental science, vol 428, no 1, p 012061
He X, Dai H, Ning P (2016) Faster learning and adaptation in security games by exploiting information asymmetry. IEEE Trans Signal Process 64(13):3429–3443
Head B (2019) Breach of faith. Co Dir 35(9):62
Hodo E, Bellekens X, Hamilton A, Tachtatzis C, Atkinson R (2017) Shallow and deep networks intrusion detection system: a taxonomy and survey. arXiv:1701.02145
Hou S, Saas A, Chen L, Ye Y (2016) Deep4maldroid: a deep learning framework for android malware detection based on linux kernel system call graphs. In: 2016 IEEE/WIC/ACM international conference on web intelligence workshops (WIW), pp 104–111
Huang X, Lu Y, Li D, Ma M (2018) A novel mechanism for fast detection of transformed data leakage. IEEE Access 6:35 926-35 936
Huang L, Joseph AD, Nelson B, Rubinstein BI, Tygar JD (2011) Adversarial machine learning. In: Proceedings of the 4th ACM workshop on security and artificial intelligence, pp 43–58
Jaggi M (2013) Revisiting Frank–Wolfe: projection-free sparse convex optimization. In: ICML (1), pp 427–435
Javaid A, Niyaz Q, Sun W, Alam M (2016) A deep learning approach for network intrusion detection system. In: Proceedings of the 9th EAI international conference on bio-inspired information and communications technologies, pp 21–26
Jiang Z, Zhao J, Li X-Y, Han J, Xi W (2013) Rejecting the attack: source authentication for wi-fi management frames using CSI information. In: Proceedings IEEE INFOCOM, pp 2544–2552

Jiang C, Zhang H, Ren Y, Han Z, Kwang KC, Lajos H (2016) Machine learning paradigms for next-generation wireless networks. IEEE Wirel Commun 24(2):98–105
Jing Q, Vasilakos AV, Wan J et al (2014) Security of the Internet of Things: perspectives and challenges. Wirel Netw 20:2481–2501
Jonathan OA, Oeldorf-Hirsch A (2020) The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. Inf Commun Soc 23(1):128–147
Kang M-J, Kang J-W (2016) Intrusion detection system using deep neural network for in-vehicle network security. PLoS ONE 11(6):e0155781
Keetharuth BS, Forbes AN, Simmons WP (2019) Increasing legal protections at the international, regional and national levels for human rights defenders working in Africa and Asia E-WEL-2016-5378, September 2016–August 2019
Khan MA, Khan S, Shams B, Lloret J (2016) Distributed flood attack detection mechanism using artificial neural network in wireless mesh networks. Secur Commun Netw 9(15):2715–2729
Kharraz A, Robertson W, Kirda E (2018) Surveylance: automatically detecting online survey scams. In: IEEE symposium on security and privacy, pp 70–86
Kömürcü G, Dündar G (2012) Determining the quality metrics for PUFs and performance evaluation of two RO-PUFs. In: 10th IEEE international NEWCAS conference, pp 73–76
Kwon D, Kim H, Kim J, Suh SC, Kim I, Kim KJ A (2017) Survey of deep learning-based network anomaly detection, cluster computing
Larriva-Novo XA, Vega-Barbas M, Villagrá VA, Rodrigo MS (2020) Evaluation of cybersecurity data set characteristics for their applicability to neural networks algorithms detecting cybersecurity anomalies. IEEE Access 8:9005–9014
Lee JH, Kim H (2017) Security and privacy challenges in the Internet of Things [Security and privacy matters]. IEEE Consum Electron Mag 6(3):134–136
Lheureux A, Grolinger K, Elyamany HF, Capretz MA (2017) Machine learning with big data: challenges and approaches. IEEE Access 5:7776–7797
Li JH (2019) Cyber security meets artificial intelligence: a survey. Front Inf Technol Electron Eng 19:1462–1474
Li W, Huang J (2018) Mobile physical layer spoofing detection based on sparse representation. IET Commun 12(14):1709–1713
Li P, Liu Q, Zhao W, Wang D, Wang S (2018) Chronic poisoning against machine learning based IDSS using edge pattern detection. In.:IEEE international conference on communications (ICC), pp 1–7
Lin Q, Tu S, Waqas M, ur Rehman S, Chang CC (2019) Tracking areas planning based on spectral clustering in small cell networks. IET Commun 13(13):1921–1927
Liu FJ, Wang X, Primak SL (2013) A two dimensional quantization algorithm for CIR-based physical layer authentication. In: IEEE international conference on communications (ICC), pp 4724–4728
Liu H, Wang Y, Liu J, Yang J, Chen Y (2014) Practical user authentication leveraging channel state information (csi). In: Proceedings of the 9th ACM symposium on information, computer and communications security, pp 389–400
Liu M, Tu S, Xiao C, Waqas M, ur Rehman S, Aamir M, Chang CC (2020a) The allocation and reuse scheme of physical cell identifications based on maximum degree first coloring algorithm. IEEE Syst J 14(1):582–591
Liu X, Lin Y, Li H, Zhang J (2020b) A novel method for malware detection on ML-based visualization technique. Comput Secur 89:101682
Liu X et al (2021) Privacy and security issues in deep learning: a survey. IEEE Access 9:4566–4593
Lobato AGP, Lopez MA, Sanz IJ, Cardenas AA, Duarte, OCM, Pujolle G (2018) An adaptive real-time architecture for zero-day threat detection. In: IEEE international conference on communications (ICC), pp 1–6
Lohstroh M (2017) Why the equifax breach should not have mattered
Lotfollahi M, Siavoshani MJ, Zade RSH, Saberian M (2017) Deep packet: a novel approach for encrypted traffic classification using deep learning. Soft Comput 24:1999–2012
Lu Y, Huang X, Ma Y, Ma M (2018a) A weighted context graph model for fast data leak detection. In: IEEE international conference on communications (ICC), pp 1–6
Lu X, Wan X, Xiao L, Tang Y, Zhuang W (2018b) Learning-based rogue edge detection in VANETs with ambient radio signals. In: IEEE international conference on communications (ICC), pp 1–6
Mahfouz AM, Venugopal D, Shiva SG (2020) Comparative analysis of ML classifiers for network intrusion detection. In: 4th international congress on information and communication technology, pp 193–207
Mao Q, Hu F, Hao Q (2018) Deep learning for intelligent wireless networks: a comprehensive survey. IEEE Commun Surv Tutor 20(4):2595–2621

Martín ML, Carro B, Sánchez-Esguevillas AJ, Mauri JL (2017) Conditional variational auto-encoder for prediction and feature recovery applied to intrusion detection in IoT. Sensors 112:2372–2381
Martinelli F, Marulli F, Mercaldo F (2017) Evaluating convolutional neural network for effective mobile malware detection. Procedia Comput Sci 112:2372–2381
McLaughlin N, Martinez del Rincon J, Kang B, Yerima S, Miller P, Sezer S, Safaei Y, Trickel E, Zhao Z, Doupé A, Joon Ahn G (2017) Deep android malware detection. In: Proceedings of the seventh ACM on data and application security and privacy, New York, NY, USA, pp 301–308
Mizuno S, Hatada M, Mori T, Goto S (2017) Botdetector: a robust and scalable approach toward detecting malware-infected devices. In: IEEE international conference on communications (ICC), pp 1–7
Moore AW, Atkeson CG (1993) Prioritized sweeping: reinforcement learning with less data and less time. Mach Learn 13(1):103–130
Narudin FA, Feizollah A, Anuar NB, Gani A (2016) Evaluation of machine learning classifiers for mobile malware detection. Soft Comput 20(1):343–357
Natalya VM (2019) Computer games to fill the gap in learning functional lexis at russian colleges and universities. In: International conference on quality management, transport and information security, information technologies, pp 639–643
Ni J, Zhang K, Vasilakos AV (2021) Security and privacy for mobile edge caching: challenges and solutions. IEEE Wirel Commun 28(3):77–83
Otoum S, Kantarci B, Mouftah HT (2019) On the feasibility of deep learning in sensor network intrusion detection. IEEE Netw Lett 1(2):68–71
Oulehla M, Oplatková ZK, Malanik D (2016) Detection of mobile botnets using neural networks. In: Future technologies conference (FTC), pp 1324–1326
Ozcelik H (2020) An analysis of fraudulent financial reporting using the fraud diamond theory perspective: an empirical study on the manufacturing sector companies listed on the Borsa Istanbul. In: Grima S, Boztepe E, Baldacchino PJ (eds) Contemporary issues in audit management and forensic accounting. Emerald Publishing Limited
Pan F, Wen H, Liao R, Jiang Y, Xu A, Ouyang K, Zhu X (2017) Physical layer authentication based on channel information and machine learning. In: IEEE conference on communications and network security (CNS), pp 364–365
Patel A, Tailor J (2020) A malicious activity monitoring mechanism to detect and prevent ransomware. Comput Fraud Secur 2020(1):14–19
Pei C, Zhang N, Shen XS, Mark JW (2014) Channel-based physical layer authentication. In: IEEE global communications conference, pp 4114–4119
Pihur UV, Korolova A (2014) Rappor: randomized aggregatable privacy-preserving ordinal response. In: Proceedings of the conference on computer and communications security. ACM, pp 1054–1067
Prasad R, Rohokale V (eds) (2020) Artificial intelligence and machine learning in cyber security. In: Cyber security: the lifeline of information and communication technology. Springer, pp 231–247
Rath M, Mishra S (2020) Security approaches in machine learning for satellite communication. Springer, Berlin, pp 189–204
Rehman S, Tu S, Waqas M, Huang Y, Rehman O, Ahmad B, Ahmad S (2019) Unsupervised pre-trained filter learning approach for efficient convolution neural networks. Neurocomputing 365:171–190
Ricci J, Breitinger F, Baggili I (2019) Survey results on adults and cybersecurity education. Educ Inf Technol 24(1):231–249
Rodríguez-Gómez RA, Maciá-Fernández G, García-Teodoro P (2013) Survey and taxonomy of botnet research through life-cycle. ACM Comput Surv 45(4):45:1-45:33
Roel M (2012) Physically unclonable functions: constructions, properties and applications. Katholieke Universiteit Leuven, Belgium
Sagduyu YE, Shi Y, Erpek T, Headley W, Flowers B, Stantchev G, Lu Z (2020) When wireless security meets machine learning: motivation, challenges, and research directions. arXiv preprint arXiv:2001.08883
Saied A, Overill RE, Radzik T (2016) Detection of known and unknown DDoS attacks using artificial neural networks. Neurocomputing 172:385–393
Shakiba-Herfeh M, Chorti A, Poor HV (2020) Physical layer security: authentication, integrity and confidentiality. arXiv:2001.07153
Sharmeen S, Ahmed YA, Huda S, Koçer B, Hassan MM (2020) Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. IEEE Access 8:24522–24534
Singar AV, Akhilesh K (2020) Role of cyber-security in higher education. In: Akhilesh KB, Möller DPF (eds) Smart technologies. Springer, pp 249–264

Siponen M, Puhakainen P, Vance A (2020) Can individuals' neutralization techniques be overcome? A field experiment on password policy. Comput Secur 88:101617
Smith SS (2020) Cybersecurity & insurance. In: Blockchain, artificial intelligence and financial services. Springer, Berlin, pp 193–200
Srinivas TAS, Somula R, Govinda K (2020) Privacy and security in Aadhaar. In: Howlett R, Jain LC (eds) Smart intelligent computing and applications. Springer, Berlin, pp 405–410
Steward D, Cavazos R (2019) Big data analytics in us courts: uses, challenges, and implications. Springer Nature, Berlin
Su X, Zhang D, Li W, Zhao K (2016) A deep learning approach to android malware feature learning and detection. In: 2016 IEEE Trustcom/BigDataSE/ISPA, pp 244–251
Sun Y, Yen GG, Yi Z (2018) Evolving unsupervised deep neural networks for learning meaningful representations. IEEE Trans Evol Comput 23(1):89–103
Sutton RS, Barto AG (1998) Introduction to reinforcement learning, vol 135. MIT Press, Cambridge
Taheri R, Ghahramani M, Javidan R, Shojafar M, Pooranian Z, Conti M (2020) Similarity-based android malware detection using Hamming distance of static binary features. Future Gener Comput Syst 105:230–247
Tam K, Feizollah A, Anuar NB, Salleh R, Cavallaro L (2017) The evolution of android malware and android analysis techniques. ACM Comput Surv 49(4):76:1-76:41
Tang TA, Mhamdi L, McLernon D, Zaidi SAR, Ghogho M (2016) Deep learning approach for network intrusion detection in software defined networking. In: International conference on wireless networks and mobile communications (WINCOM), pp 258–263
Tanveer M, Abbas G, Abbas ZH, Waqas M, Muhammad F, Kim S (2020) S6AE: securing 6LoWPAN using authenticated encryption scheme. Sensors 20(9):2707
Tello-Oquendo L, Pacheco-Paramo D, Pla V, Martinez-Bauset J (2018) Reinforcement learning-based ACB in LTE-A networks for handling massive M2M and H2H communications. In: IEEE international conference on communications (ICC), pp 1–7
Thing VLL (2017) IEEE 802.11 network anomaly detection and attack classification: a deep learning approach. In: 2017 IEEE wireless communications and networking conference (WCNC), pp 1–6
Thomas T, Vijayaraghavan AP, Emmanuel S (2020) Adversarial machine learning in cybersecurity. In: Machine learning approaches in cybersecurity analytics. Springer, Berlin, pp 185–200
Tomasin S (2018) Analysis of channel-based user authentication by key-less and key-based approaches. IEEE Trans Wirel Commun 17(9):5700–5712
Torres P, Catania C, Garcia S, Garino CG (2016) An analysis of recurrent neural networks for botnet detection behavior. In: IEEE Biennial Congress of Argentina (ARGENCON), pp 1–6
Tu S, Liu M, Waqas M, Rehman S, Zhu R, Liu L (2018a) FHC-PCIA: a physical cell identification allocation method based on fuzzy hierarchical clustering for heterogeneous cellular network. IEEE Access 6:46976–46987
Tu S, Huang X, Huang Y, Waqas M, Rehman SU (2018b) SSLSS: semi-supervised learning-based steganalysis scheme for instant voice communication network. IEEE Access 6:66 153-66 164
Tu S, Waqas M, Rehman SU, Aamir M, Rehman OU, Jianbiao Z, Chang C-C (2018c) Security in fog computing: a novel technique to tackle an impersonation attack. IEEE Access 6:74 993-75 001
Tu S, Waqas M, Meng Y, Rehman S, Ahmad I, Koubaa A, Halim Z, Hanif M, Chang CC, Shi C (2020a) Mobile fog computing security: a user-oriented smart attack defense strategy based on DQL. Comput Commun 160:790–798
Tu S, Rehman S, Waqas M, Rehman O, Yang Z, Ahmad B, Halim Z, Zhao W (2020b) Optimisation-based training of evolutionary convolution neural network for visual classification applications. IET Comput Vis 14(5):259–267
Tu S et al (2021) Reinforcement learning assisted impersonation attack detection in device-to-device communications. IEEE Trans Veh Technol 70(2):1474–1479
Tugnait JK (2013) Wireless user authentication via comparison of power spectral densities. IEEE J Sel Areas Commun 31(9):1791–1802
Valdeón RA (2019) Ad hoc corpora and journalistic translation research: BBC News and BBC Mundo's coverage of Margaret Thatcher's death and funeral. Across Lang Cult 20(1):79–95
Viganò E, Loi M, Yaghmaei E (2020) Cybersecurity of critical infrastructure. In: Christen M, Gordijn B, Loi M (eds) The ethics of cybersecurity. The international library of ethics, law and technology, vol 21. Springer, Cham
Wan X, Xiao L, Li Q, Han Z (2017) Fhy-layer authentication with multiple landmarks with reduced communication overhead. In: IEEE international conference on communications (ICC), pp 1–6
Wang Z (2015) The applications of deep learning on traffic identification, BlackHat USA, vol 24

Wang H, Yeung DY (2016) Towards Bayesian deep learning: a framework and some existing methods. IEEE Trans Knowl Data Eng 28(12):3395–3408
Wang N, Jiang T, Lv S, Xiao L (2017) Physical-layer authentication based on extreme learning machine. IEEE Commun Lett 21(7):1557–1560
Waqas M, Zeng M, Li Y (2017) Mobility-assisted device-to-device communications for content transmission. In: 13th international wireless communications and mobile computing conference (IWCMC), pp 206–211
Waqas M, Ahmed M, Li Y, Jin D, Chen S (2018a) Social-aware secret key generation for secure device-to-device communication via trusted and non-trusted relays. IEEE Trans Wirel Commun 17(6):3918–3930
Waqas M, Niu Y, Ahmed M, Li Y, Jin D, Han Z (2018b) Mobility-aware fog computing in dynamic environments: understandings and implementation. IEEE Access 7:38867–38879
Waqas M, Zeng M, Li Y, Jin D, Han Z (2018c) Mobility assisted content transmission for device-to-device communication underlaying cellular networks. IEEE Trans Veh Technol 67(7):6410–6423
Waqas M, Ahmed M, Zhang J, Li Y (2018d) Confidential information ensurance through physical layer security in device-to-device communication. In: IEEE global communications conference (GLOBECOM), pp 1–7
Waqas M, Niu Y, Li Y, Ahmed M, Jin D, Chen S, Han Z (2020a) A comprehensive survey on mobility-aware D2D communications: principles, practice and challenges. IEEE Commun Surv Tutor 22(3):1863–1886
Waqas M, Tu S, Rehman S, Halim Z, Anwar S, Abbas G, Abbas ZH (2020b) Authentication of vehicles and road side units in intelligent transportation system. Comput Mater Contin: CMC 64(1):359–371
Weinand A, Karrenbauer M, Sattiraju R, Schotten H (2017) Application of machine learning for channel based message authentication in mission critical machine type communication. In: European wireless; 23th European wireless conference, pp 1–5
Winfield A (2019) Ethical standards in robotics and AI. Nat Electron 2(2):46
Wu P, Guo H, Moustafa N (2020) Pelican: a deep residual network for network intrusion detection. In: 50th annual IEEE/IFIP international conference on dependable systems and networks workshops (DSN-W), pp 55–62
Xiao L, Greenstein L, Mandayam N, Trappe W (2007) Fingerprints in the ether: using the physical layer for wireless authentication. In: IEEE international conference on communications, pp 4646–4651
Xiao L, Li Y, Liu G, Li Q, Zhuang W (2015) Spoofing detection with reinforcement learning in wireless networks. In: IEEE global communications conference (GLOBECOM), pp 1–5
Xiao L, Li Y, Han G, Liu G, Zhuang W (2016a) PHY-layer spoofing detection with reinforcement learning in wireless networks. IEEE Trans Veh Technol 65(12):10037–10047
Xiao L, Chen T, Han G, Zhuang W, Sun L (2016b) Channel-based authentication game in MIMO systems. In: IEEE global communications conference (GLOBECOM), pp 1–6
Xiao L, Chen T, Han G, Zhuang W, Sun L (2017) Game theoretic study on channel-based authentication in MIMO systems. IEEE Trans Veh Technol 66(8):7474–7484
Xiao L, Wan X, Han Z (2018a) Phy-layer authentication with multiple landmarks with reduced overhead. IEEE Trans Wirel Commun 17(3):1676–1687
Xiao L, Li Y, Dai C, Dai H, Poor HV (2018b) Reinforcement learning-based NOME power allocation in the presence of smart jamming. IEEE Trans Veh Technol 67(4):3377–3389
Xiao L, Wan X, Su W, Tang Y (2018c) Anti-jamming underwater transmission with mobility and learning. IEEE Commun Lett 22(3):542–545
Xiao L, Jiang D, Xu D, Zhu H, Zhang Y, Poor HV (2018d) Two-dimensional anti-jamming mobile communication based on reinforcement learning. IEEE Trans Veh Technol 67(10):9499–9512
Xiao L, Zhuang W, Zhou S, Chen C (2019) Learning-based rogue edge detection in VANETs with ambient radio signals. In: Shen XS (ed) Learning-based VANET communication and security techniques. Springer, pp 13–47
Xu Z, Liu W, Huang J, Yang C, Lu J, Tan H (2020) Artificial intelligence for securing IoT services in edge computing: a survey. Secur Commun Netw 2020:8872586
Yang L, Lau L, Gan H (2020) Investors' perceptions of the cybersecurity risk management reporting framework. Int J Account Inf Manag 28(1):167–183
Yousefi-Azar M, Varadharajan V, Hamey L, Tupakula U (May 2017) Autoencoder-based feature learning for cybersecurity applications. In: International joint conference on neural networks (IJCNN), pp 3854–3861

Yu M-D, Sowell R, Singh A, M'Raïhi D, Devadas S (2012) Performance metrics and empirical results of a PUF cryptographic key generation ASIC. In: IEEE international symposium on hardware-oriented security and trust, pp 108–115

Yuan Z, Lu Y, Wang Z, Xue Y (2014) Droid-sec: deep learning in android malware detection. SIGCOMM Comput Commun Rev 44(4):371–372

Yuan Z, Lu Y, Xue Y (2016) Droiddetector: android malware characterization and detection using deep learning. Tsinghua Sci Technol 21(1):114–123

Yuan S, Li L, Chigan C (2018) Maximum mean discrepancy based secure fusion strategy for robust cooperative spectrum sensing. In: IEEE international conference on communications (ICC), pp 1–6

Zaidi K, Milojevic MB, Rakocevic V, Nallanathan A, Rajarajan M (2016) Host-based intrusion detection for VANETs: a statistical approach to rogue node detection. IEEE Trans Veh Technol 65(8):6703–6714

Zeng M, Li Y, Zhang K, Waqas M, Jin D (2018) Incentive mechanism design for computation offloading in heterogeneous fog computing: a contract-based approach. In: IEEE international conference on communications (ICC), pp 1–6

Zhang Z, Ning H, Shi F, Farha F, Xu Y, Xu J, Zhang F, Choo KKR (2021) Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artif Intell Rev

Zheng Z, Xie S, Dai H-N, Chen W, Chen X, Weng J, Imran M (2020) An overview on smart contracts: challenges, advances and platforms. Future Gener Comput Syst 105:475–491

Zhou L, Pan S, Wang J, Vasilakos AV (2017a) Machine Learning on big data: opportunities and challenges. Neurocomputing 237:350–361

Zhou T, Cai Z, Xiao B, Chen Y, Xu M (2017b) Detecting rogue AP with the crowd wisdom. In: IEEE 37th international conference on distributed computing systems (ICDCS), pp 2327–2332

Zong W, Chow Y-W, Susilo W (2020) Interactive three-dimensional visualization of network intrusion detection data for machine learning. Future Gener Comput Syst 102:292–306

Zou Y, Zhu J, Wang X, Hanzo L (2016) A survey on wireless security: technical challenges, recent advances, and future trends. Proc IEEE 104(9):1727–1765