Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 3 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i03.50727

PAPER

Deep Reinforcement Learning-Based Framework for Enhancing Cybersecurity

Malek M. Al-Nawashi[1](✉), Obaida M. Al-hazaimeh[1,2], Nedal M. Tahat[3], Nasr Gharaibeh[1], Waleed A. Abu-Ain[4], Tarik Abu-Ain[5]

[1]Al-Huson University College, Al-Balqa Applied University, Irbid, Jordan

[2]Faculty of Information Technology, Department of Information Security and Cybersecurity, Philadelphia University, Amman, Jordan

[3]Faculty of Science, The Hashemite University, Zarqa, Jordan

[4]College of Science and Computer Engineering, Taibah University, Yanbu, Saudi Arabia

[5]College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

nawashi@bau.edu.jo

ABSTRACT

The detection of cyberattacks has been increasingly emphasized in recent years, focusing on both infrastructure and people. Conventional security measures such as intrusion detection, firewalls, and encryption are insufficient in protecting cyber systems against growing and changing threats. In order to address this problem, scholars have explored reinforcement learning (i.e., RL) as a potential solution for intricate cybersecurity decision-making difficulties. Nevertheless, the use of RL faces several obstacles, including dynamic attack scenarios, insufficient training data, and the challenge of replicating real-world complexities. This study presents a novel framework that uses deep reinforcement learning (i.e., DRL) to simulate harmful cyberattacks and improve cybersecurity. This study presents an agent-based framework that is capable of ongoing learning and adaptation in a dynamic network security environment. The agent determines the optimal course of action by considering the current state of the network and the rewards it receives for its decisions. The CIC-IDS-2018 database, constructed using Python 3.7 programming, was used. The conducted studies yielded outstanding results, with a detection accuracy of 98.82% achieved for the CIC-IDS-2018 database in cyberattack classification.

KEYWORDS

Internet of Things (IoT), deep reinforcement learning (DRL), cybersecurity, network security, machine learning (ML)

1 INTRODUCTION

A wide variety of industries have made extensive use of Internet of Things (IoT) technology, including but not limited to transportation, manufacturing, healthcare, education, government, water and power management, finance, and entertainment. The IoT has enabled previously unimaginable levels of functionality and user service thanks to the integration of numerous information and communication technology (ICT) tools. In the past ten years, there has been tremendous progress in ICT with regard to intelligence devices, network architecture, and system design. For instance,

Al-Nawashi, M.M., Al-hazaimeh, O.M., Tahat, N.M., Gharaibeh, N., Abu-Ain, W.A., Abu-Ain, T. (2025). Deep Reinforcement Learning-Based Framework for Enhancing Cybersecurity. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(3), pp. 170–190. https://doi.org/10.3991/ijim.v19i03.50727

Article submitted 2024-06-24. Revision uploaded 2024-10-29. Final acceptance 2024-10-30.

advancements in cognitive radio networks and 5G cellular networks, software-defined networks (SDNs), cloud computing, and other related technologies have elevated ICT. These advances increase vulnerability to cyberattacks, which are attempts by one or more computers to attack network infrastructures, computer information systems, or personal computer devices. Economic competitors or state-sponsored adversaries may launch electronic attacks [1]. To reduce the impact of these attacks, cybersecurity systems must be developed [2, 3]. Figure 1 illustrates a few of the services and features that the IoT provides [4].

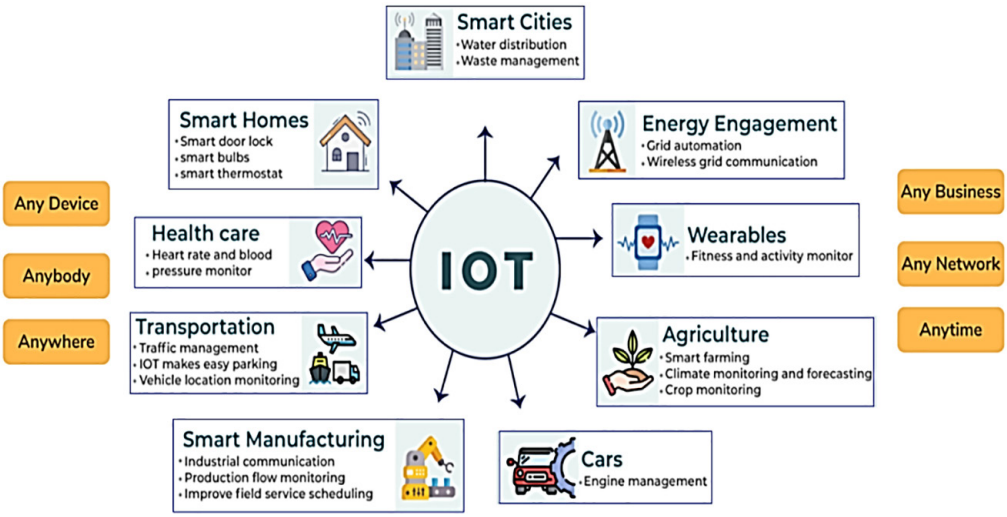

Fig. 1. IoT applications and services

Both offensive and defensive strategies have been implemented in cyberspace using artificial intelligence (AI), with a particular emphasis on machine learning (ML). ML is applied by the attackers in order to compromise protection methods. When it comes to cyber-security, ML is utilized to establish a strong defense against security threats. This is done in order to prevent and minimize the effects of any damages or impacts that may occur [5]. One of the most common uses of ML is the detection of intrusions, malware, data privacy protection, and cyber-physical attacks [6, 7]. Unsupervised and supervised learning approaches have been utilized extensively in these applications. While supervised methods learn by examples based on the labels of the data, unsupervised approaches, in principle, investigate the patterns and structure of the data without making use of the labels. Unfortunately, these methods cannot respond dynamically and sequentially to cyberattacks, especially new or emerging threats. Detection and defense generally occur after attacks, when traces can be collected and analyzed, hindering proactive security options. Statistics suggest that 65% of attacks were detected after causing significant cyber system damage [8, 9]. Figure 2 illustrates the diverse varieties of cybersecurity attacks. Consequently, it is imperative to establish efficient strategies for identifying these attacks prior to their inflicting substantial harm on the cyber system [10, 11].

Reinforcement learning (RL), a subfield of ML, closely resembles human learning as it acquires knowledge from its own experiences by actively exploring and exploiting unfamiliar environments [12]. RL can be used to create an independent agent that can make optimal sequential decisions, even without much prior knowledge of the environment. This makes RL very adaptive and valuable in real-time and adversarial environments. By using function approximation and representation

learning, deep learning (DL) has been integrated into RL techniques, allowing them to effectively tackle a wide range of intricate issues [13, 14].

Fig. 2. Various types of cyberattacks

The integration of RL and DL makes them highly suitable for cybersecurity applications, as cyber threats are becoming more complex, quick, and widespread [15]. To clarify, ML is an essential element of AI, and Figure 3 illustrates the links between various subfields [16].

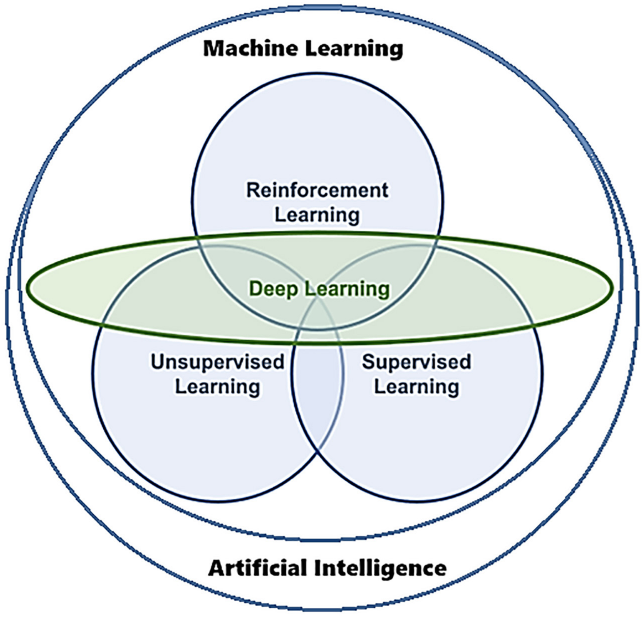

Fig. 3. Relationship between AI, ML, RL, unsupervised, supervised, and DL

Estimating complex functions from high-dimensional inputs is the ultimate objective of deep reinforcement learning (DRL), which employs a neural network. By using DL, conventional RL methods are enhanced to capture the massive scale of numerous networked systems, including IoT devices and wireless networks [17]. For the purpose of this study, DRL is utilized to improve the security of the IoT by classifying and detecting different kinds of cyberattacks that IoT networks may be subjected to. These threats include data reconnaissance attacks, distributed denial of service attacks (DDOS), and distributed denial of service (DOS) attacks. Essentially, the main contributions of this study are to highlight the benefits of DRL and to suggest it as a viable substitute for traditional ML models. The paper is organized as follows: Related works are examined in Section 2. The dataset employed in the experiments is delineated in Section 3. RL, DL, and DRL are all introduced in Section 4. The proposed DRL model is comprehensively described in Section 5. Section 6 presents the simulation results and evaluation, while Section 7 offers conclusions.

2 RELATED WORK

The techniques and methods pertinent to the DRL method, particularly the method for detecting cyber-attacks from IoT traffic, are extensively discussed in this portion of the literature. Caminero et al. [18] investigated the use of various DRL algorithms for intrusion detection on the NSL-KDD and AWID datasets. These algorithms include DDQN, PG, and actor-critic framework. Alavizadeh et al. [19] suggested a methodology for detecting network intrusions that combines deep feed-forward neural network with RL. The model has the ability to independently acquire knowledge in a network setting and detect different instances of unauthorized access by employing an automated method of experimentation and learning from mistakes. The empirical findings in this study are derived from the NSL-KDD dataset. Randhawa et al. [20] propose a generative adversarial network (GAN) framework enhanced with DRL to explore the production of semantically consistent samples. A DRL agent is employed to confront the discriminator of the GAN, which serves as a detector for Botnets. The discriminator is taught using the deliberate perturbations generated by the agent during the GAN training process. The GAN generator is implemented to expedite convergence compared to cases where DRL is not utilized. Borchjes et al. [21], when it comes to software denied network cybersecurity, the authors contrast neural episodic control with double-deep Q-networks (DQNs). Both algorithms appear to be effective means of network defense, according to the data. Since the two methods are essentially interchangeable, the simplicity of DDQN makes it the better choice. Dutta et al. [22] employing DRL to defend against strategic multi-stage attacks. The DRL defense agent learns network and multi-stage attack patterns to compute context-aware defensive tactics while reducing system effects. Effective management of power operations and automatic recognition of cyberattacks are the goals of the Dragon DRL approach, which was created by Landen et al. [23], which intends to improve the capabilities of attack detection and autonomous grid operation. For the purpose of DRAGON's performance evaluation, the researchers simulated different assault scenarios using the IEEE 14-Bus power transmission system paradigm. Table 1 contains a list of publications that have been published in this field.

Table 1. Relevant studies-communication networks

Reference	Description	Domain	Method	Year
Al-Rawi et al. [24]	This study summarizes the use of RL-based routing algorithms in wireless distributed networks. We have identified the problems, benefits, and performance gains that RL has brought to several routing methods.	Routing – Wireless Networks	Reinforcement Learning	2015
Althamary et al. [25]	Reviewing the applications of MARL, this allows decentralized and scalable decision making in shared contexts. The paper summarizes various challenges linked to vehicular networks.	MARL – Vehicular Networks	Reinforcement Learning	2019
Cui et al. [26]	This survey summarizes ML methods and their applications, focusing on supervised and unsupervised ML solutions for the Internet of Things (i.e., IoT).	IoT	Machine Learning	2018
Luong et al. [27]	This study surveys the existing research on DRL approaches, expansions, and applications for solving various communications and networking problems.	Networking and Communications	Deep Reinforcement Learning	2019
Nguyen et al. [28]	There has been a review of the many technical obstacles to multi-agent learning, along with their remedies and examples of their use to address practical issues through the use of DRL techniques.	Multi-agent Systems – MAS	Deep Reinforcement Learning	2020
Lei et al. [6]	This paper provides an overview of the AIoT systems, which are structured into three layers: the perception layer, the network layer, and the application layer. The categorization of DRL-AIoT applications and the incorporation of RL components for each tier have been summarized.	IoT – Autonomous	Deep Reinforcement Learning	2020
Kumar et al. [29]	This study reviewed ML-based WSN algorithms (including RL approaches) from 2014 to March 2018. The many WSN challenges and the benefits of using ML techniques have been discussed.	WSN	Machine Learning and Reinforcement Learning	2019
Da Costa et al. [30]	This article examines the methods of intrusion detection for IoT security and the ML techniques that are used to address these issues.	IoT – Security	Machine Learning	2023
Wang et al. [31]	Cognitive radio networks' RL-based Dynamic Spectrum Access (i.e., DSA) algorithms have been categorized.	Networks for Cognitive Radio – DSA	Machine Learning	2022

Deep reinforcement learning has been extensively adopted across a variety of application domains as a result of the rapid advancements in software and distributed computing [27]. Table 2 provides a summary of the most common applications of DRL in cybersecurity attacks, as well as a selection of publications in each category.

Table 2. Most common applications of DRL in cybersecurity attacks

Reference	Application	Algorithms	Action
Akazaki et al. [32]	Reinforced CPS falsification	A3C and Double DQN	Select an input signal from a list of piecewise constants to use as the next input value.
Xiao et al. [33]	Wireless network spoofing detection	Dyna-Q and Q-learning	The action set has a range of discrete authentication threshold values that can be chosen from within a given interval.
Gupta et al. [34]	Improving autonomous system defenses against attackers	Trust Region Policy optimization – TRPO	Find the appropriate estimating rule to turn a corrupted state into an estimated state.
Ferdowsi et al. [35]	Autonomous vehicle safety and security	Q-learning with LSTM	Use appropriate velocities to ensure that there is a safe distance between AVs.

(Continued)

Table 2. Most common applications of DRL in cybersecurity attacks *(Continued)*

Reference	Application	Algorithms	Action
Han et al. [36]	Communication technique that prevents jamming for CRN	CNN-using DQN	Actions are taken by SUs to either select a frequency channel to transmit signals or to exit a geographical area where smart jammers are blocking transmissions.
Chatterjee et al. [37]	Phishing detection with automated URLs	DQN	For each URL, choose 0 for safe and 1 for malicious.
Wan et al. [38]	Offloading mobile processes to the cloud for malware detection	DQN and Hot-booting Q-learning	Find the best offloading rate for every mobile device.
Xiao et al. [39]	Method for safe mobile crowd sensing	DQN	For mobile users, choose the best payment method for the server.

3 DATASET

There are several datasets that are accessible to the general public on the Internet, with a particular emphasis on IoT traffic. Table 3 is a presentation of the information regarding the three-label datasets that are the most widely used [40].

Table 3. Most common datasets

Dataset	Description	Size (Record)		Year	Attacks	Availability
		Training	Testing			
NSL_KDD	Duplicated data in the standard KDD99 network traffic dataset can hurt the training model. Tavallaee et al. [41] created the NSL-KDD dataset to address this issue. The KDD dataset is more rational and improves model training performance by removing superfluous information and adjusting data quantity in the training and testing sets [42].	125973	22544	2009	DOS, probe, U2R, and R2L attacks	Publically available
AWID	There are three attacks on IEEE 802.11 networks included in the Aegean Wi-Fi Intrusion Dataset (AWID), which also includes regular network traffic [43].	1795574	575642	2016	Data reconnaissance attacks, DDoS, and DOS attack	Publically available
CSE-CIC-IDS 2018	The University of New Brunswick initially developed this dataset for the purpose of evaluating DDoS data. This dataset was exclusively obtained from the year 2018 and will not receive any further updates. The dataset was derived from the server logs of the university [44].	6311436	1577859	2018	DDoS, web, DoS, brute force, botnet, and Heartbleed attacks	Publically available

To assess the effectiveness of DRL, we employed the CSE-CIC-IDS-2018 dataset in this study to classify two label values; normal and anomalous. These labels are used to identify various types of cyber threats that IoT networks may encounter.

4 REINFORCEMENT LEARNING

Deep learning, reinforcement learning, and DRL are all introduced in this section. We will delve into the fundamental concepts, techniques, and applications of each

field, thereby establishing a strong foundation for comprehending these sophisticated branches of artificial intelligence.

4.1 Reinforcement learning

Reinforcement learning involves a learner or agent embedded in an environment that must improve its actions in response to each state or environmental situation as shown in Figure 4. Critically, unlike supervised learning, the agent does not receive clear feedback on right actions. Instead, every action produces a signal indicating the presence or absence of a reward, and the problem in RL is to continuously adjust behavior in order to maximize the accumulated reward over time. Since the agent is not explicitly instructed on what actions to take, it must engage in exploration and gather information about the results of different acts. Through this process, it gradually develops a behavioral policy that maximizes rewards [45]. A learning algorithm or the design of the learning system is not the defining factors in RL; rather, it is the learning problem that matters. Truly, numerous designs and algorithms have been created, covering a broad spectrum of assumptions about the quantities that are represented, how they are updated based on experience, and decision-making processes [38].

An essential aspect of solving any RL problem is determining the optimal method of representing the state of the environment. In the initial stages of research on RL, the focus was on uncomplicated environments with a limited number of potential states. The agents involved were basic and learned about each state individually, using what is known as a tabular state representation. This type of representation is inherently limited in its ability to support generalization, which is the capacity to apply knowledge gained about one state to other similar states. This limitation becomes more pronounced as environments grow larger and more intricate, and individual states are less likely to repeat [46].

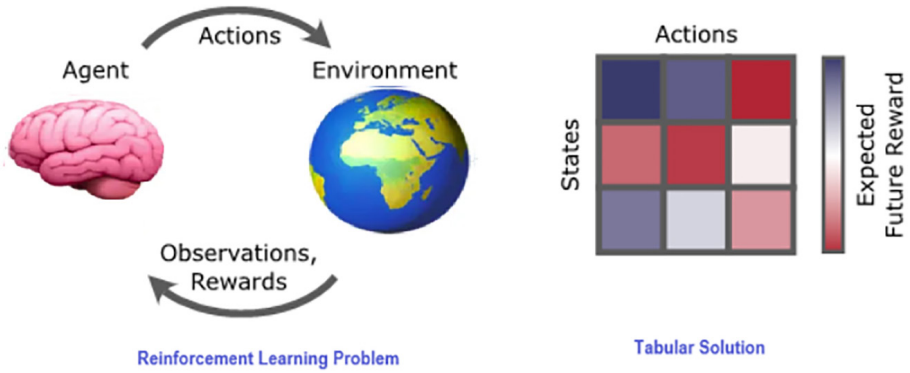

Fig. 4. Reinforcement learning

4.2 Deep learning

Deep neural networks are complex computational systems consisting of units that resemble neurons, which are interconnected through contacts that resemble synapses, as shown in Figure 5. Each unit sends a scalar value, similar to a spike rate that is calculated by adding up its inputs. The inputs are the activities of "upstream"

units multiplied by the strength of the transmitting synapse or link. Significantly, the activity of a unit is not directly proportional to its inputs, which means that networks with multiple layers of units placed between the input and output sides of the system (known as "deep" neural networks) can approximate any function that maps activation inputs to activation outputs. Moreover, in neural networks with loops, such as "recurrent" neural networks, the network's activations can retain knowledge about previous events, enabling the network to perform computations based on sequences of inputs [47].

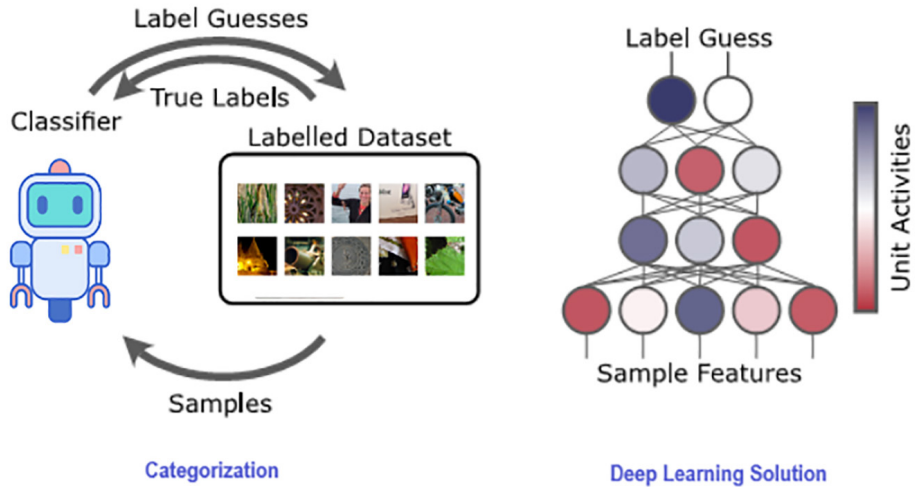

Fig. 5. Deep learning

"Deep Learning" is the process of fitting a desired input-output mapping into a deep neural network by modifying its connection weights. With its use of the chain rule from calculus, backpropagation determines how to modify weights throughout a network and is thus the most efficient and popular algorithm for handling this problem [48].

4.3 Deep reinforcement learning

Deep reinforcement learning utilizes the expressive capabilities of DL to address the challenge of RL. A DRL system is characterized as a system that effectively solves a RL problem by utilizing representations that are acquired through training a deep neural network, rather than being predetermined by the creator [23]. DRL systems commonly employ a deep neural network to calculate a non-linear transformation from perceptual inputs to action values or action probabilities. These systems also utilize RL signals to update the weights in the network, often through backpropagation. This updating process aims to improve the accuracy of reward estimates or to increase the occurrence of highly rewarded actions, as depicted in Figure 6 [6].

An early example of successful DRL may be seen in the 1990s with the development of TD-Gammon. This system, which utilized neural networks and RL, was able to learn how to play backgammon at a competitive level against skilled human players. TD-Gammon employed a temporal difference RL method that calculated a state-value estimate for each encountered board position, indicating the system's likelihood of winning. The algorithm subsequently calculated a reward-prediction error (RPE),

which serves as an indicator of positive surprise or disappointment based on the following events. The RPE was utilized as an error signal in the backpropagation process, which adjusted the weights of the network to produce more precise state-value predictions. Choose actions to maximize state value for the following board state. For several training games, TD-Gammon used self-play, where the algorithm played against itself until one side won [7, 46, 49, 50].

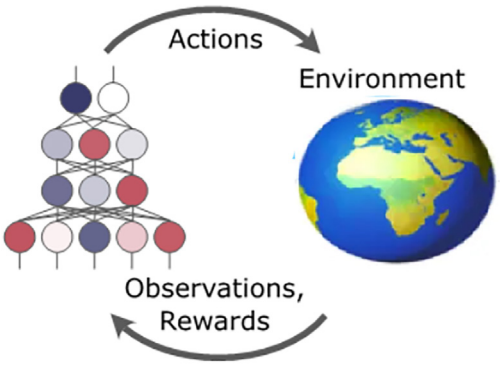

Fig. 6. Deep reinforcement learning

In this study, DRL is utilized to enhance security by classifying and identifying cyber threats on IoT networks, taking advantage of its previously described benefits. These threats include data reconnaissance attacks, DDoS attacks, and DoS attacks. This study highlights the advantages of DRL and suggests it as a feasible substitute for ML models. Figure 7 illustrates the applications of DRL for network security and IoT [27].

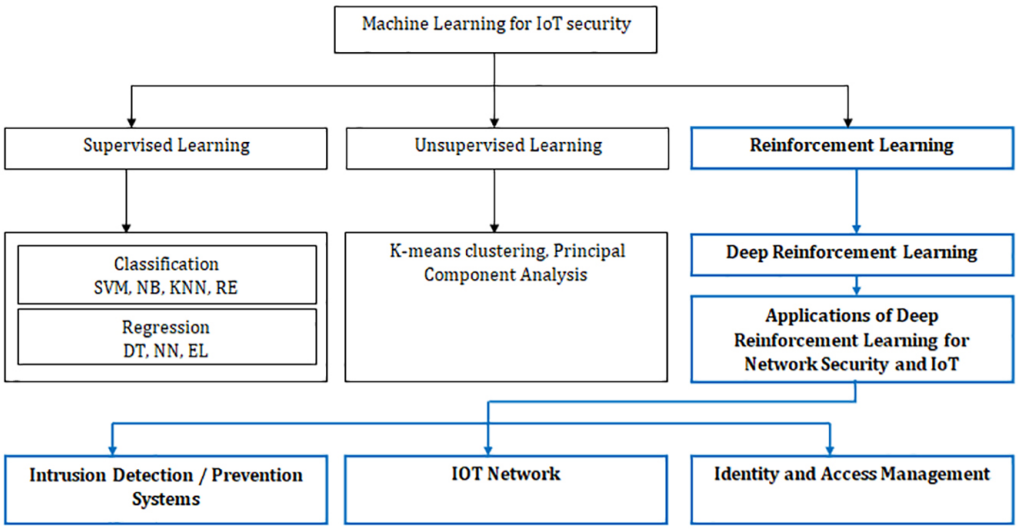

Fig. 7. Applications of deep reinforcement learning for network security and IoT

5 PROPOSED DEEP REINFORCEMENT LEARNING MODELS

A novel cyber defense framework is proposed in this paper to reduce the effects of cybersecurity attacks through the use of cyberattacks. In Figure 8, we present a block diagram of the architecture of our proposed framework.

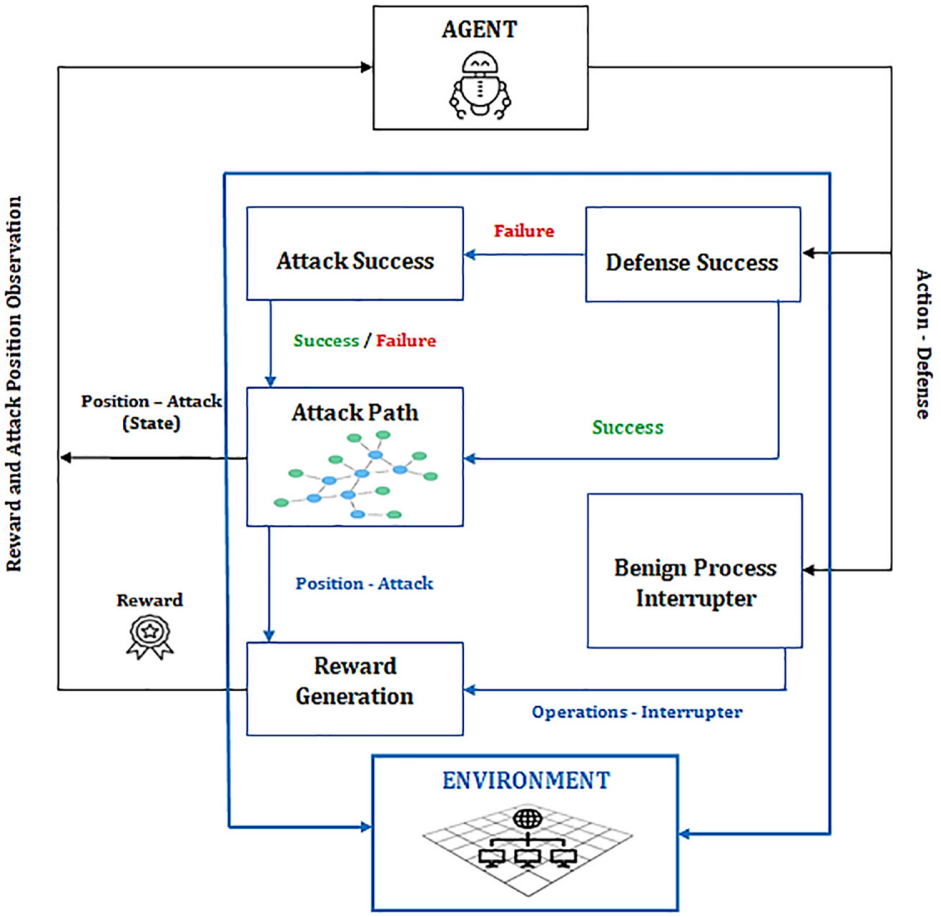

Fig. 8. Proposed framework

A custom OpenAI gym [51] simulation environment that we developed is the fundamental component of our framework. In this environment, a DRL defense agent executes a defense action at each time-sequence and observes the attack position and reward as feedback. An attack path is considered in each episode, which consists of multiple time sequences. The adversary and defense models within the proposed framework are comprehensively described in the subsequent subsections.

5.1 Adversary model

The adversary's objective is to progressively transition from the reconnaissance tactic to the impact tactic. If one of their techniques is executed effectively, the adversary employs a logic-based model to accomplish the objective of a particular tactic. From the reconnaissance point to the impact position, the attacker has a lot of options depending on their attack method. Based on what we know about the effects of past attacks and the current state of the network and system, we presume that an adversary can adjust their tactics. Consequently, they can find the deployed countermeasures and avoid or defeat any static defense scheme. The effective execution of an attack relies on the adversary taking use of one or more vulnerabilities that have not yet been patched. These vulnerabilities may be unknown or blocked from being patched due to concerns regarding usability, safety, or stability.

5.2 Defense model

The primary goal of the defender (DRL agent) is to proactively obstruct the adversary from reaching the Impact tactic phase, while simultaneously minimizing the loss resulting from the interruption of benign operations. The agent must predict the next attack action and infer the current attack position in order to determine the optimal defense. Nevertheless, the defender is unable to develop an a priori system dynamics model due to the absence of domain-specific information regarding system complexities and adversarial behavior, as illustrated in Table 4.

Table 4. Restrictions of dynamic modeling-uncertainties

Uncertain	Description
Next Attack Procedure	Lack of domain data prevents the defensive agent from knowing the next attack method or its possibility.
Next Attack Technique	There are two reasons why the defense agent fails to predict the next attack method. To begin with, the defense agent is in the dark about the attack's structure because it calls for difficult-to-obtain, real-world attack sequences, domain-specific. Secondly, the tactic (attack sequence) used by an adversary could change at any time.
Incomplete Observations	The effectiveness of deployed alert mechanisms in determining the current position of the adversary may be hindered by two factors: (1) the restricted ability to observe processes, and (2) the uncertainty in mapping observations to specific attack strategies.

5.3 State

The state S_t at any discrete time step in DRL is a critical input for decision-making algorithms, as it encapsulates the complete configuration of the environment. Formally, the state $S_t \in S$ evolves according to the dynamics Markovian particles (i.e., DMP) described by the probability distribution $\boldsymbol{P}(S_t + 1 \mid S_t, a_t)$ where $a_t \in A$ is the action taken by the agent at time t. The agent's objective is to derive an optimal policy π^*: $S \rightarrow A$ that maximizes the expected discounted return $\boldsymbol{E}\left[\sum_{k=0}^{\infty} \gamma^k r_t + k + 1 \mid S_t, a_t\right]$. Thus, the state optimizes the agent's performance in the long run by guiding its learning process dynamically.

5.4 Action

The actions $a_t \in A$ that the agent selects at discrete time step t are a critical component of the decision-making process in DRL. These actions directly influence the subsequent state $S_t + 1$ in accordance with the stochastic transition dynamics $\boldsymbol{P}(S_t + 1 \mid S_t, a_t)$. The agent's strategy, formalized as a policy $\pi(a_t \mid s_t)$ intended to optimize the anticipated cumulative reward. Consequently, the action a_t is a critical decision variable that guides the agent through the state space in order to maximize the returns of the long term.

5.5 Reward function

In DRL, the reward function measures the immediate and long-term rewards that an agent obtains for its actions in specific states. This function guides the agent

to improve its behavior over time based on a policy. As a reward function for the defense agent, we take into consideration:

$$R_t = \boldsymbol{E}\left[\sum_{k=0}^{\infty}\gamma^k r_t + k + 1 \mid S_t, a_t\right] \quad (1)$$

where, the variable $r_t + k + 1$ represents the reward that is obtained at the time step $t + k + 1$, S_t, a_t indicates the expected value given the present state S_t and action a_t, and the discount factor γ, sometimes known as gamma, is a variable between 0 and 1 that defines the current value of rewards that will be received in the future.

6 SIMULATION AND EVALUATION

In this section, we conduct simulations to evaluate the effectiveness of our framework and existing works.

6.1 Simulation setup

For this study, we utilized the CSE-CIC-IDS-2018 dataset to evaluate the proposed framework's performance in classifying instances into two label values: normal and anomalous. These labels are utilized to categorize different kind of cyberattacks that IoT networks may encounter (DDoS). In addition, we provide the following performance metrics to evaluate the predictive capabilities of the various models: accuracy, F1 score, recall, and precision. The definitions of these performance measures are derived from well-recognized standards. The equations for each metric are presented in Table 5 [52–56].

Table 5. Metrics evaluation – equations

Metric	Equation	
F1 score	$= 2 * \frac{Precision * Recall}{Recall + Precision}$	(2)
Accuracy	$= \frac{TN + TP}{TN + TP + FN + FP}$	(3)
Precision	$= \frac{TN + TP}{TP + FP} * 100$	(4)
Recall	$= \frac{TP}{TP + FN} * 100$	(5)

The proposed DRL algorithm was implemented using the RLlib library in Python 3.7 for experiment design. In our simulations, we employed an HP laptop that was equipped with an Intel(R) Core 2.40 GHz Intel Core i5-1135G7 processor, 8GB of RAM, and three 4GB NVIDIA GM200 graphics cards.

6.2 Simulation results

An adaptive decoy placement strategy is generated by our system using a DRL algorithm, as indicated earlier. In Figure 9, we can see the DRL agent's training

performance plotted. The simulation results indicate that the framework is scalable and performs successfully in terms of convergence time.

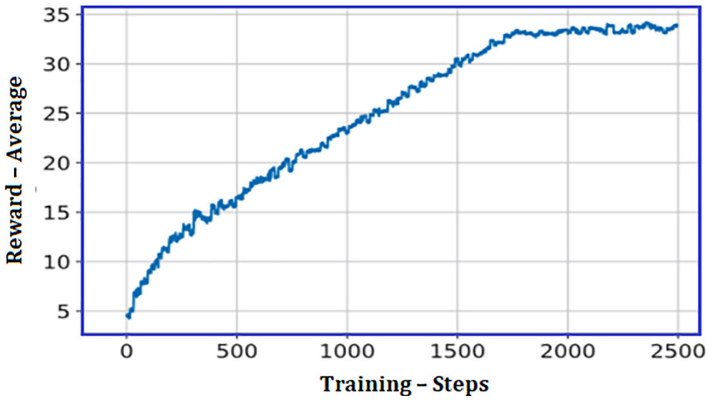

Fig. 9. Training process

The proposed framework results were examined when it was applied to the CSE-CIC-IDS-2018 dataset. The data was divided into two sets: a testing set, which accounted for 20% of the dataset, and a training set, which accounted for 80% of the dataset. Stratifying the dataset was an option to guarantee uniform percentages across all classes. Table 6 calculates and lists the evaluation metrics of the proposed framework. Subsequently, the outcome is depicted in the column chart, as illustrated in Figure 10.

Table 6. Results of the evaluation metrics-proposed framework

Metric	Categories – Attacks	
	DDoS	Benign
Accuracy	98.07	98.82
F1-score	92.58	98.92
Precision	86.64	98.35
Recall	99.62	98.27

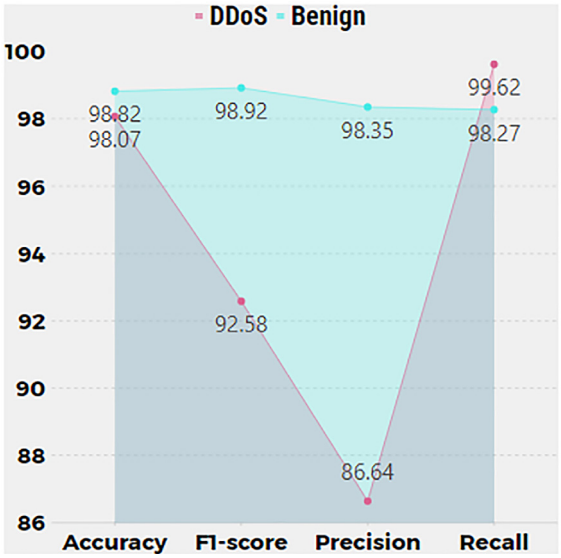

Fig. 10. Evaluation metrics-column chart

The findings indicate the accuracy of predicting attacks for the two categories in the confusion matrix, as shown in Figure 11.

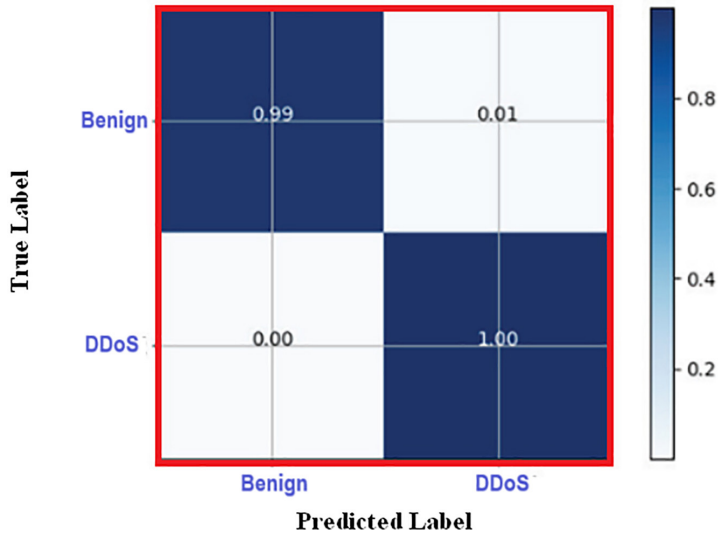

Fig. 11. The confusion matrix in the proposed framework—CSE-CIC-IDS2018

Our proposed framework facilitates the automated identification and protection against cyberattacks, resulting in enhanced effectiveness in detecting and defending against IoT cyberattacks. The suggested framework exhibits a high level of recall, specifically 99.62% for DDoS and 98.27% for benign. The results indicate a significant level of accuracy, with a precision of 86.64% for DDoS and 98.35% for benign. The results indicate a substantial F1-score of 92.58% for DDoS and 98.92% for benign, as well as a high accuracy of 98.07% for DDoS and 98.82% for benign. Table 7 provides a clear comparison between the proposed model and a selection of existing methods (i.e., state-of-the-art), also known as the state of the art. Subsequently, the outcome is depicted in the column chart, as illustrated in Figure 12.

Table 7. Comparative analysis with previous studies—proposed framework

Reference	Method	Datasets	Accuracy – (%)	F1-Score – (%)	Precision – (%)	Recall – (%)
Lopez-Martin et al. [58]	DDQN	NSL-KDD	89.78	91.20	89.44	93.03
		AWID	95.70	93.94	92.35	95.70
Otoum et al. [59]	SDPN	NSL-KDD	96.02	97.14	95.38	96.91
Alavizadeh et al. [19]	DQL	NSL-KDD	78.07	81.41	77.84	76.76
Tuan et al. [60]	Unsupervised Learning	UNBS-NB 15	97.08	–	–	91.88
Dong et al. [61]	DDQN	NSL-KDD	73.43	69.02	66.61	–
		AWID	96.47	96.73	97.40	–
Alaghbari et al. [62]	AE-CNN	N-BaIoT	97.00	94.00	94.00	93.00
Ren et al. [63]	DDQN	CIC_IDS	94.11	92.51	–	–
Proposed Framework	DRL	CIC-IDS	98.07	92.58	86.64	99.62

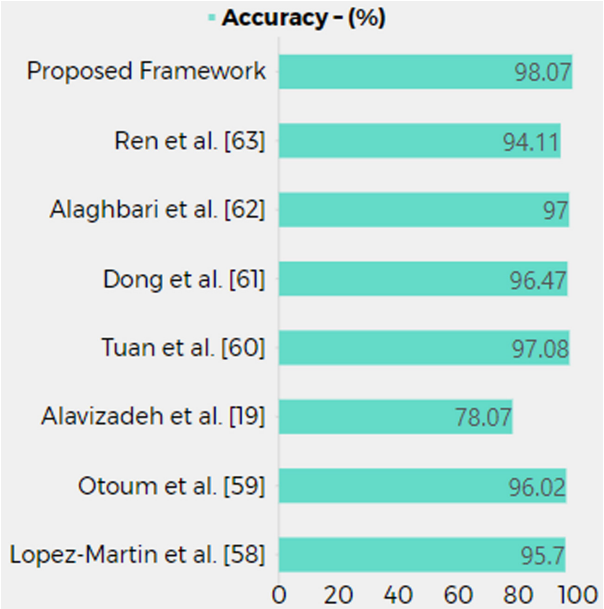

Fig. 12. State of the art – comparative analysis

Accuracy is the primary metric employed in algorithm comparisons for cybersecurity applications to assess an algorithm's ability to identify and protect against attacks in real-world scenarios [64–68]. For the reasons delineated in Table 7, the proposed method demonstrates superior accuracy in comparison to specific existing methods. This suggests that it is a practical alternative for the detection and defense of cyberattacks.

7 CONCLUSION

The proposed framework interacts with the network using RL. DRL agents autonomously gather and analyze network data to detect malicious payloads. Additionally, the proposed DRL model, along with other RL models, reduces prediction times, making them ideal for online detection and current network applications. To improve learning, we investigate DRL agent parameters such as the number of learning episodes, discount factor, and batch size to find the best fine-tuning strategies for network cyberattack detection. The suggested DRL framework can autonomously categorize different network threats with great accuracy, proving its learning capability. Future work (our next effort), includes cloud implementation of our proposed solution. This deployment will improve the DRL agent's self-learning and real-time threat classification. The constraint of this study is real-world cybersecurity scenarios encompass extensive networks, endpoints, devices, and attacks. Rapidly identifying optimal policies poses challenges for DRL agents because of their intricate action space. The cybersecurity landscape is dynamic, complicating the learning process, and CIC-IDS-2018, such as with most databases, fails to encompass all cyberattacks. Numerous notable attack strategies, including DoS, DDoS, brute force, botnets, and web-based methods. To facilitate the identification of optimal policies in future endeavors, streamline the action space of DRL agents.

8 CONFLICT OF INTEREST

The authors confirm that they have no affiliations with or involvement in any organization or entity that has a financial or non-financial interest in the subject matter or materials discussed in this manuscript.

9 REFERENCES

[1] M. Afshari, K. A. Bakar, W. S. Luan, B. A. Samah, and F. S. Fooi, "Factors affecting teachers' use of information and communication technology," *International Journal of Instruction,* vol. 2, pp. 77–104, 2009.

[2] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects," *Electronics,* vol. 11, no. 9, p. 1502, 2022. https://doi.org/10.3390/electronics11091502

[3] A. H. K. Mohammed, H. Jebamikyous, D. Nawara, and R. Kashef, "IoT cyber-attack detection: A comparative analysis," in *International Conference on Data Science, E-learning and Information Systems 2021*, 2021, pp. 117–123. https://doi.org/10.1145/3460620.3460742

[4] X. Xiaojiang, W. Jianli, and L. Mingdong, "Services and key technologies of the Internet of Things," *Zte Communications,* vol. 8, pp. 26–29, 2020.

[5] J. Martínez Torres, C. Iglesias Comesaña, and P. J. García-Nieto, "Machine learning techniques applied to cybersecurity," *International Journal of Machine Learning and Cybernetics,* vol. 10, pp. 2823–2836, 2019. https://doi.org/10.1007/s13042-018-00906-1

[6] L. Lei, Y. Tan, K. Zheng, S. Liu, K. Zhang, and X. Shen, "Deep reinforcement learning for autonomous internet of things: Model, applications and challenges," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 3, pp. 1722–1760, 2020. https://doi.org/10.1109/COMST.2020.2988367

[7] A. Chowdhury, S. A. Raut, and H. S. Narman, "DA-DRLS: Drift adaptive deep reinforcement learning based scheduling for IoT resource management," *Journal of Network and Computer Applications,* vol. 138, pp. 51–65, 2019. https://doi.org/10.1016/j.jnca.2019.04.010

[8] A. Sharma, Z. Kalbarczyk, J. Barlow, and R. Iyer, "Analysis of security data from a large computing organization," in *2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN)*, 2011, pp. 506–517. https://doi.org/10.1109/DSN.2011.5958263

[9] O. M. Al-Hazaimeh, N. Alhindawi, and N. A. Otoum, "A novel video encryption algorithm-based on speaker voice as the public key," in *2014 IEEE International Conference on Control Science and Systems Engineering*, 2014, pp. 180–184. https://doi.org/10.1109/CCSSE.2014.7224533

[10] M. A. Vander–Pallen, P. Addai, S. Isteefanos, and T. K. Mohd, "Survey on types of cyber attacks on operating system vulnerabilities since 2018 onwards," in *2022 IEEE World AI IoT Congress (AIIoT)*, 2022, pp. 1–7. https://doi.org/10.1109/AIIoT54504.2022.9817246

[11] O. M. Al-Hazaimeh, "A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 5, pp. 4824–4834, 2020. https://doi.org/10.11591/ijece.v10i5.pp4824-4834

[12] S. K. Sahu, A. Mokhade, and N. D. Bokde, "An overview of machine learning, deep learning, and reinforcement learning-based techniques in quantitative finance: Recent progress and challenges," *Applied Sciences,* vol. 13, no. 3, p. 1956, 2023. https://doi.org/10.3390/app13031956

[13] L. Buşoniu, T. De Bruin, D. Tolić, J. Kober, and I. Palunko, "Reinforcement learning for control: Performance, stability, and deep approximators," *Annual Reviews in Control*, vol. 46, pp. 8–28, 2018. https://doi.org/10.1016/j.arcontrol.2018.09.005

[14] T. M. Moerland, J. Broekens, and C. M. Jonker, "Emotion in reinforcement learning agents and robots: A survey," *Machine Learning*, vol. 107, pp. 443–480, 2018. https://doi.org/10.1007/s10994-017-5666-0

[15] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: A comprehensive survey," *The Journal of Defense Modeling and Simulation*, vol. 19, no. 1, pp. 57–106, 2022. https://doi.org/10.1177/1548512920951275

[16] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of artificial intelligence and machine learning in smart cities," *Computer Communications*, vol. 154, pp. 313–323, 2020. https://doi.org/10.1016/j.comcom.2020.02.069

[17] W. Chen, B. Zhu, K. Chi, and S. Zhang, "DRL based offloading of industrial IoT applications in wireless powered mobile edge computing," *IET Communications*, vol. 16, no. 9, pp. 951–962, 2022. https://doi.org/10.1049/cmu2.12397

[18] G. Caminero, M. Lopez-Martin, and B. Carro, "Adversarial environment reinforcement learning algorithm for intrusion detection," *Computer Networks*, vol. 159, pp. 96–109, 2019. https://doi.org/10.1016/j.comnet.2019.05.013

[19] H. Alavizadeh, H. Alavizadeh, and J. Jang-Jaccard, "Deep Q-learning based reinforcement learning approach for network intrusion detection," *Computers*, vol. 11, no. 3, p. 41, 2022. https://doi.org/10.3390/computers11030041

[20] R. H. Randhawa, N. Aslam, M. Alauthman, M. Khalid, and H. Rafiq, "Deep reinforcement learning based evasion generative adversarial network for botnet detection," *Future Generation Computer Systems*, vol. 150, pp. 294–302, 2024. https://doi.org/10.1016/j.future.2023.09.011

[21] L. Borchjes, C. Nyirenda, and L. Leenen, "Model-free deep reinforcement learning in software-defined networks," *arXiv preprint arXiv:2209.01490*, 2022.

[22] J. Orr and A. Dutta, "Multi-agent deep reinforcement learning for multi-robot applications: A survey," *Sensors*, vol. 23, no. 7, p. 3625, 2023. https://doi.org/10.3390/s23073625

[23] M. Landen, K. Chung, M. Ike, S. Mackay, J.-P. Watson, and W. Lee, "DRAGON: Deep reinforcement learning for autonomous grid operation and attack detection," in *Proceedings of the 38th Annual Computer Security Applications Conference*, 2022, pp. 13–27. https://doi.org/10.1145/3564625.3567969

[24] H. A. Al-Rawi, M. A. Ng, and K.-L. A. Yau, "Application of reinforcement learning to routing in distributed wireless networks: A review," *Artificial Intelligence Review*, vol. 43, pp. 381–416, 2015. https://doi.org/10.1007/s10462-012-9383-6

[25] I. Althamary, C.-W. Huang, and P. Lin, "A survey on multi-agent reinforcement learning methods for vehicular networks," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019, pp. 1154–1159. https://doi.org/10.1109/IWCMC.2019.8766739

[26] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, and J. Qin, "A survey on application of machine learning for Internet of Things," *International Journal of Machine Learning and Cybernetics*, vol. 9, pp. 1399–1417, 2018. https://doi.org/10.1007/s13042-018-0834-5

[27] N. C. Luong *et al.*, "Applications of deep reinforcement learning in communications and networking: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3133–3174, 2019. https://doi.org/10.1109/COMST.2019.2916583

[28] T. T. Nguyen, N. D. Nguyen, and S. Nahavandi, "Deep reinforcement learning for multiagent systems: A review of challenges, solutions, and applications," *IEEE transactions on cybernetics*, vol. 50, no. 9, pp. 3826–3839, 2020. https://doi.org/10.1109/TCYB.2020.2977374

[29] D. P. Kumar, T. Amgoth, and C. S. R. Annavarapu, "Machine learning algorithms for wireless sensor networks: A survey," *Information Fusion,* vol. 49, pp. 1–25, 2019. https://doi.org/10.1016/j.inffus.2018.09.013

[30] K. A. Da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Computer Networks,* vol. 151, pp. 147–157, 2019. https://doi.org/10.1016/j.comnet.2019.01.023

[31] Y. Wang, Z. Ye, P. Wan, and J. Zhao, "A survey of dynamic spectrum allocation based on reinforcement learning algorithms in cognitive radio networks," *Artificial Intelligence Review,* vol. 51, pp. 493–506, 2019. https://doi.org/10.1007/s10462-018-9639-x

[32] T. Akazaki, S. Liu, Y. Yamagata, Y. Duan, and J. Hao, "Falsification of cyber-physical systems using deep reinforcement learning," in *Formal Methods, FM 2018,* in Lecture Notes in Computer Science, K. Havelund, J. Peleska, B. Roscoe, and E. de Vink, Eds., Springer, Cham, vol. 10951, 2018, pp. 456–465. https://doi.org/10.1007/978-3-319-95582-7_27

[33] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Transactions on Vehicular Technology,* vol. 65, no. 12, pp. 10037–10047, 2016. https://doi.org/10.1109/TVT.2016.2524258

[34] A. Gupta and Z. Yang, "Adversarial reinforcement learning for observer design in autonomous systems under cyber attacks," *arXiv preprint arXiv:1809.06784,* 2018.

[35] A. Ferdowsi, U. Challita, W. Saad, and N. B. Mandayam, "Robust deep reinforcement learning for security and safety in autonomous vehicle systems," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018, pp. 307–312. https://doi.org/10.1109/ITSC.2018.8569635

[36] G. Han, L. Xiao, and H. V. Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017, pp. 2087–2091. https://doi.org/10.1109/ICASSP.2017.7952524

[37] M. Chatterjee and A.-S. Namin, "Detecting phishing websites through deep reinforcement learning," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, 2019, pp. 227–232. https://doi.org/10.1109/COMPSAC.2019.10211

[38] X. Wan, G. Sheng, Y. Li, L. Xiao, and X. Du, "Reinforcement learning based mobile offloading for cloud-based malware detection," in *GLOBECOM 2017–2017 IEEE Global Communications Conference*, 2017, pp. 1–6. https://doi.org/10.1109/GLOCOM.2017.8254503

[39] L. Xiao, Y. Li, G. Han, H. Dai, and H. V. Poor, "A secure mobile crowdsensing game with deep reinforcement learning," *IEEE Transactions on Information Forensics and Security,* vol. 13, no. 1, pp. 35–47, 2017. https://doi.org/10.1109/TIFS.2017.2737968

[40] A. Alshaibi, M. Al-Ani, A. Al-Azzawi, A. Konev, and A. Shelupanov, "The comparison of cybersecurity datasets," *Data,* vol. 7, no. 2, p. 22, 2022. https://doi.org/10.3390/data7020022

[41] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009, pp. 1–6. https://doi.org/10.1109/CISDA.2009.5356528

[42] A. Özgür and H. Erdem, "A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015," *PeerJ Preprints,* vol. 4, pp. 1–21, 2016. https://doi.org/10.7287/peerj.preprints.1954

[43] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 1, pp. 184–208, 2015. https://doi.org/10.1109/COMST.2015.2402161

[44] R. B. Basnet, R. Shash, C. Johnson, L. Walgren, and T. Doleck, "Towards detecting and classifying network intrusion traffic using deep learning frameworks," *J. Internet Serv. Inf. Secur.,* vol. 9, pp. 1–17, 2019.

[45] Z. Ding, Y. Huang, H. Yuan, and H. Dong, "Introduction to reinforcement learning," in *Deep Reinforcement Learning: Fundamentals, Research and Applications*, H. Dong, Z. Ding, and S. Zhang, Eds., 2020, pp. 47–123. https://doi.org/10.1007/978-981-15-4095-0_2

[46] S. Rawas and A. D. Samala, "Revolutionizing brain tumor analysis: A fusion of chatGPT and multi-modal CNN for unprecedented precision," *International Journal of Online & Biomedical Engineering (iJOE),* vol. 20, no. 8, pp. 37–48, 2024. https://doi.org/10.3991/ijoe.v20i08.47347

[47] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. MIT Press, 2018.

[48] S. Mahadevan and M. Maggioni, "Learning representation and control in markov decision processes: New frontiers," *Journal of Machine Learning Research*, vol. 8, 2007. https://doi.org/10.1561/9781601982391

[49] H. Li, D. Liu, and D. Wang, "Manifold regularized reinforcement learning," *IEEE Transactions on Neural Networks and Learning Systems,* vol. 29, no. 4, pp. 932–943, 2017. https://doi.org/10.1109/TNNLS.2017.2650943

[50] K. Nahar, O. Al-Hazaimeh, A. Abu-Ein, and N. Gharaibeh, "Phonocardiogram classification based on machine learning with multiple sound features," *Journal of Computer Science,* vol. 16, no. 11, pp. 1648–1656, 2020. https://doi.org/10.3844/jcssp.2020.1648.1656

[51] O. Al-hazaimeh, S. A. Alomari, J. Alsakran, and N. Alhindawi, "Cross correlation–new based technique for speaker recognition," *Int J Acad Res,* vol. 6, pp. 232–239, 2014. https://doi.org/10.7813/2075-4124.2014/6-3/A.33

[52] W. Qiang and Z. Zhongli, "Reinforcement learning model, algorithms and its application," in *2011 International Conference on Mechatronic Science, Electric Engineering and Computer (MEC),* 2011, pp. 1143–1146. https://doi.org/10.1109/MEC.2011.6025669

[53] O. M. Al-Hazaimeh, M. Al-Nawashi, and M. Saraee, "Geometrical-based approach for robust human image detection," *Multimedia Tools and Applications,* vol. 78, pp. 7029–7053, 2019. https://doi.org/10.1007/s11042-018-6401-y

[54] N. Gharaibeh, O. M. Al-Hazaimeh, B. Al-Naami, and K. M. Nahar, "An effective image processing method for detection of diabetic retinopathy diseases from retinal fundus images," *International Journal of Signal and Imaging Systems Engineering,* vol. 11, no. 4, pp. 206–216, 2018. https://doi.org/10.1504/IJSISE.2018.093825

[55] M. Al-Nawashi, O. M. Al-Hazaimeh, and M. Saraee, "A novel framework for intelligent surveillance system based on abnormal human activity detection in academic environments," *Neural Computing and Applications,* vol. 28, pp. 565–572, 2017. https://doi.org/10.1007/s00521-016-2363-z

[56] O. M. Al-Hazaimeh and M. Al-Smadi, "Automated pedestrian recognition based on deep convolutional neural networks," *International Journal of Machine Learning and Computing (IJMLC),* vol. 9, no. 5, pp. 662–667, 2019. https://doi.org/10.18178/ijmlc.2019.9.5.855

[57] O. M. Al-Hazaimeh and A. Ma'moun, "Vehicle to vehicle and vehicle to ground communication-speech encryption algorithm," in *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 2023, pp. 1–4. https://doi.org/10.1109/ICECCME57830.2023.10252814

[58] M. Lopez-Martin, B. Carro, and A. Sanchez-Esguevillas, "Application of deep reinforcement learning to intrusion detection for supervised problems," *Expert Systems with Applications,* vol. 141, p. 112963, 2020. https://doi.org/10.1016/j.eswa.2019.112963

[59] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: A deep learning–based intrusion detection framework for securing IoT," *Transactions on Emerging Telecommunications Technologies,* vol. 33, no. 3, 2022. https://doi.org/10.1002/ett.3803

[60] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, and N. T. K. Son, "Performance evaluation of Botnet DDoS attack detection using machine learning," *Evolutionary Intelligence,* vol. 13, pp. 283–294, 2020. https://doi.org/10.1007/s12065-019-00310-w

[61] P. Dong, Z.-M. Chen, X.-W. Liao, and W. Yu, "A deep reinforcement learning (DRL) based approach for well-testing interpretation to evaluate reservoir parameters," *Petroleum Science,* vol. 19, no. 1, pp. 264–278, 2022. https://doi.org/10.1016/j.petsci.2021.09.046

[62] K. A. Alaghbari, H.-S. Lim, M. H. M. Saad, and Y. S. Yong, "Deep autoencoder-based integrated model for anomaly detection and efficient feature extraction in IoT networks," *IoT,* vol. 4, no. 3, pp. 345–365, 2023. https://doi.org/10.3390/iot4030016

[63] M. Ren, R. Xu, and T. Zhu, "Double deep Q-Network decoder based on EEG brain-computer interface," *ZTE Communications,* vol. 21, p. 3, 2023.

[64] M. M. Al-Nawashi, O. M. Al-hazaimeh, I. S. Al-Qasrawi, A. A. Abu-Ein, and M. H. Al-Bsool, "Analysis and evolution of SHA-1 algorithm – analytical technique," *International Journal of Computer Networks & Communications (IJCNC),* vol. 16, no. 3, pp. 89–101, 2024. https://doi.org/10.5121/ijcnc.2024.16306

[65] N. Tahat, O. M. Al-hazaimeh, and S. Shatnawi, "A new authentication scheme based on chaotic maps and factoring problems," in *Mathematics and Computation, IACMC 2022, Springer Proceedings in Mathematics & Statistics*, D. Zeidan, J. C. Cortés, A. Burqan, A. Qazza, J. Merker, and G. Gharib, Eds., Springer, Singapore, vol. 418, 2023, pp. 53–64. https://doi.org/10.1007/978-981-99-0447-1_5

[66] R. Shaqbou'a, N. Tahat, O. Ababneh, and O. M. Al-Hazaimeh, "Chaotic map and quadratic residue problems-based hybrid signature scheme," *International Journal for Computers & Their Applications,* vol. 29, 2022.

[67] A. Obaida, M. Al-Jamal, M. Bawaneh, N. Alhindawi, and B. Hamdoni, "A new image encryption scheme using dual chaotic map synchronization," *International Arab Journal of Information Technology,* vol. 18, no. 1, pp. 95–102, 2021. https://doi.org/10.34028/iajit/18/1/11

[68] O. M. Al-hazaimeh, M. A. Al-Shannaq, M. J. Bawaneh, and K. M. Nahar, "Analytical approach for data encryption standard algorithm," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 14, pp. 126–143, 2023. https://doi.org/10.3991/ijim.v17i14.38641

10 AUTHORS

Malek M. Al-Nawashi is an Assistant Professor in the Department of Computer Science and Information Technology at Al-Balqa Applied University–Al-huson University College, Jordan. He has completed his Ph.D at University of Salford Manchester in Computer Science in 2019. His main research interests are image processing and machine learning. He can be contacted at email: nawashi@bau.edu.jo.

Obaida M. Al-Hazaimeh earned B.Sc. in Computer Science from Jordan's Applied Science University in 2004 and M.Sc. in Computer Science from Malaysia's University Science Malaysia in 2006. In 2010, he earned Ph.D in Network Security (Cryptography) from Malaysia. He is a Full Professor at Al-Balqa Applied University's Department of Computer Science and Information Technology. Cryptology, image processing, machine learning, and chaos theory are among his primary research interests. He has published around 60 papers in international refereed publications as an author or co-author. He can be contacted at email: dr_obaida@bau.edu.jo.

Nedal M. Tahat received his BSc in Mathematics at the Yarmouk University, Jordan, in 1994, and MSc in Pure Mathematics at Al al-Bayt University, Jordan, in 1998. He is a Ph.D in Applied Number Theory (Cryptography) from the National

University of Malaysia (UKM), in 2010. He is a Full Professor at the Department Mathematics, the Hashemite University. His main research interests are cryptology and number theory. He has published 57 papers, authored/co-authored, and more than 15 refereed journal and conference papers. He can be contacted at email: nedal@hu.edu.jo.

Nasr Gharaibeh is an Assistance Professor in the Department of electrical Engineering at Al-Balqa Applied University – Al-huson University College, Jordan. He received his Ph.D in Electronic engineering in 2000. He can be contacted at email: nas@bau.edu.jo.

Waleed A. Abu-Ain did his Ph.D in Artificial Intelligence in 2016 from the Artificial Intelligence Technology Center of the National University of Malaysia, Department of Computer Science (UKM). Since 2016, he is working as a full-time Assistant Professor in the Department of Computer Science at Taibah University, Applied College, Saudi Arabia. His research interests include artificial intelligence, machine learning and optimization, data science, computer vision, deep learning, and the Internet of Things. He can be contacted at email: wabuain@taibahu.edu.sa.

Tarik Abu-Ain holds a Ph.D. in Computer Science from the National University of Malaysia (UKM), Malaysia. He is an Assistant Professor in the Department of Computer Science, College of Computing and Informatics, Saudi Electronic University, KSA. His current research interests include image processing, machine learning, artificial intelligence, document image analysis, computer and wireless networking, and network security.