Hindawi
Security and Communication Networks
Volume 2022, Article ID 4996427, 9 pages
https://doi.org/10.1155/2022/4996427

Research Article

Privacy-Enhanced Intrusion Detection and Defense for Cyber-Physical Systems: A Deep Reinforcement Learning Approach

Qingyuan Lin,[1] **Rui Ming**,[2] **Kailing Zhang**,[1] **and Haibo Luo**[2]

[1]*Guangxi University of Science and Technology, Liuzhou, China*
[2]*Minjiang University, Fuzhou, China*

Correspondence should be addressed to Haibo Luo; robhappy@qq.com

Received 31 August 2022; Revised 21 September 2022; Accepted 30 September 2022; Published 10 October 2022

Academic Editor: Yulei Wu

Cyber-physical systems (CPSs) will play an important role in future real-world applications through the deep integration of computing, communication, and control technologies. CPSs are increasingly deployed in critical infrastructure, industry, and homes to achieve a smart grid, smart transportation, and smart healthcare and to bring many benefits to citizens, businesses, and governments. However, the openness and complexity brought by network and wireless communication technology, as well as the intelligence and dynamic of network intrusions make CPS more vulnerable to network intrusions and bring more serious threats to human life, enterprise productivity, and national security. Therefore, intrusion detection and defense in CPS have attracted considerable attention and have become a fundamental aspect of CPS security. However, a new challenging problem arises: how to improve the efficiency and accuracy of intrusion detection while protecting user privacy during the intrusion detection process. To address this challenge, we propose a deep reinforcement learning-based privacy-enhanced intrusion detection and defense mechanism (PIDD) for CPS. The PIDD is composed of three modules: privacy-enhanced topology graphs generation module, graph convolutional networks-based user evaluation module, and the deep reinforcement learning-based intruder identification and handling module. The experimental results show that the proposed PIDD achieves excellent performance in intrusion detection accuracy, intrusion defense percentage, and privacy protection.

1. Introduction

Cyber-physical systems (CPSs) are integral and complex systems that deeply integrate computing, communication, and physical systems. They bring a number of benefits to citizens, businesses, and governments and have attracted more attention in recent years. CPS plays an important role in wide real-world applications and has been making great business impacts in various industrial sectors, such as energy, transportation, healthcare, and manufacturing. With the rapid evolution of wireless communication networks, more and more CPS subsystems are built and connected through the communication networks, which enables more and more devices to link to CPS. However, the extensive utilization of devices with security vulnerabilities and unprotected communication networks makes CPS more prone to malicious cyber attacks and intrusions [1] (see Figure 1). These cyber threats, if they cannot be detected quickly and adjust the proper response strategy, will lead to grave consequences such as equipment damage, financial losses, and public safety. Traditional intrusion detection systems, primarily designed for conventional information technology systems, are not enough for CPS since they do not take into account the physical side of CPS.

In order to overcome these security threats, a deep reinforcement learning-based privacy-enhanced intrusion detection and defense mechanism (PIDD) is proposed for CPS. Intrusion detection and defense (IDD) is one of the most important strategy for securing CPS from malicious intrusions [2–4]; it can effectively minimize or prevent the

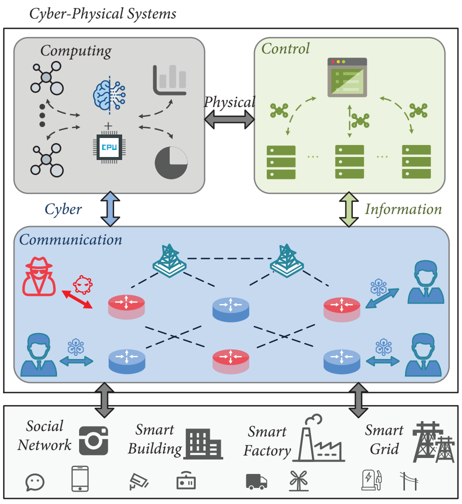


Figure 1: The architecture of cyber-physical systems and the potential security threat.

damage caused by the intrusions through performing IDD to model and monitor the malicious behaviors and intrusions early, and taking proper counter-intrusion measures and mitigation actions. With the characteristics of predicting future intrusions or security threats by building detection-based models and predictions based on empirical data, machine learning has been introduced into IDD to enhance CPS's security.

Although there are emerging machine learning-based IDD mechanisms [5–9], they do not take into account the users' privacy preservation while realizing intrusion detection and defense. Moreover, they do not combine the potential relationship between a user being an intruder and the user's communication topology graphs and features into IDD design in CPS, which helps to make the countermeasures against intrusions more efficient and reliable. The formal description of the intrusion detection problem addressed in this paper is as follows. Under the given communication conditions, it can efficiently discover intrusion behaviors and realize privacy protection at the same time.

Inspired by the previous work [10] on anomaly detection, we utilize the deep neural network with DRL training to solve the challenging problem of intrusion detection and defense in CPS. The main contributions of this paper are listed as follows.

(i) To achieve efficient intrusion detection while considering user privacy protection, we apply a variational graph autoencoder to construct a privacy-enhanced intrasystem communication topology graph and an intersystem communication topology graph with normal node characteristics. Based on these privacy-enhancing graphs and noisy node features, we employ graph convolutional networks to evaluate users' communications as regular users, intrasystem intruders, or intersystem intruders.

(ii) In order to improve the accuracy of intrusion detection, the deep reinforcement learning method twin delayed deep deterministic policy gradient algorithm (TD3) is used, which integrates the decisions made by each variational graph autoencoder during intrasystem communication and intersystem communication, respectively to determine whether the user is ultimately an intruder. Although adding noise will affect the detection accuracy, the TD3 algorithm still guarantees high-accuracy intrusion detection.

(iii) In order to effectively prevent intrusion, the corresponding countermeasures against intrusion are proposed. For intrasystem intruders, intrasystem communication is restricted, while intersystem intruders prohibit intersystem communication. In addition, both intrasystem communication and intersystem communication are prohibited for intrasystem and intersystem intruders.

(iv) Validation experiments are performed on the "CSE-CIC-IDS2018" dataset. The experimental results show that the proposed PIDD achieves excellent performance in terms of high intrusion detection accuracy, defense capability, and low privacy leakage.

The remainder of this paper is organized as follows. The proposed intrusion detection and defense framework are described in the following section. The implementation details of the DRL-based privacy-enhanced solution are then presented. Simulation results are presented and then discussed. The final section concludes this paper.

2. Overall Design of the DRL-Based Privacy-Enhanced Intrusion Detection and Defense in CPS

In this section, we first introduce the basic concept of CPS and the formulation of the intrusions and defenses problem. The proposed PIDD framework is then presented in detail.

2.1. Cyber-Physical Systems. A CPS is a controllable, reliable, and scalable multidimensional complex system that deeply integrates computing, communication, and control capabilities based on environmental perception. CPS connects physical equipment to the Internet and realizes deep integration and real-time interaction through the feedback loop of the mutual influence of computing and physical processes to add or expand new functions and detect or control physical equipment in a safe, reliable, efficient, and real-time manner. CPS enables physical devices to have five functions: computing, communication, precise control, remote coordination, and autonomy. Through the organic integration and in-depth collaboration of computation, communication, and control technologies, realtime perception, dynamic control, and information services of large-scale engineering systems are realized, which makes CPS play an important role in wide real-world applications and has been making great business impacts in various industrial sectors, such as energy, transportation, healthcare, and manufacturing.

However, the diversity of application scenarios, the openness and complexity of networking and wireless communication, and the intelligence and dynamics of intrusions bring about unpredicted security and privacy protection challenges to intrusion detection and defense mechanisms. Therefore, efficient, accurate, and privacy-enhanced intrusion detection and defense mechanisms are crucial to the success of CPS.

2.2. Intrusions and Defenses in CPS: Problem Formulation.

Cyber-intrusions mainly include intrasystem intrusions and intersystem intrusions, both of which will lead to equipment damage, economic loss, public safety, and other serious consequences. Many traditional countermeasures have been proven efficient against various intrusions. For example, in [11], to authenticate user equipment, Cui et al. first developed an edge computing-enabled unified authentication framework with the consideration of privacy preservation. Then, to prevent compromised user equipments (UEs) from launching internal intrusions, they adopt reinforcement learning and design a trust evaluation-based method to detect compromised user equipment. To enhance traditional intrusion detection mechanisms, Shen et al. [12] measure the data response processing time in the interlayer, analyze network traffic to eliminate abnormal packets, and design a hybrid augmented device fingerprinting approach to eventually realize intrusion classification and detection. However, these traditional intrusion detection systems, primarily designed for conventional information technology systems, are not enough for CPS since they do not take into account the physical side of CPS.

In recent years, as one of the important strategies to protect CPS from malicious intrusions, intrusion detection and defense have been paid attention to by theoretical research and industrial applications.

In [13], a novel intrusion detection method based on network topology verification was proposed to improve the security of the controller area network with a flexible data rate network. The method reliably detected external intrusion devices through a simple random walk-based network topology construction and subsequent verification and triggered a security mode to further protect the network from attacks. To deal with intrusion detection based on dynamic data, Qi et al. [9] proposed a new anomaly detection method combining locality-sensitive hashing, isolation forest, and PCA. This method operated on multifaceted data by introducing locality-sensitive hashing and PCA, effectively captured group anomalies and could perform model updates and processe data in constant memory and time. In [14], the vulnerabilities of in-vehicle and external networks were first discussed, and a multilayer hybrid intrusion detection algorithm, including signature-based and anomaly-based intrusion detection, was proposed to detect known and unknown attacks on in-vehicle networks.

Yang et al. [15] formulated the fine-grained known/unknown intrusion detection problem as a two-stage minimization problem, where the first stage used a conditional autoencoder to seek a score metric to minimize the empirical risk of misclassifying known attacks. The second stage was to use extreme value theory to model the distribution of reconstruction errors to find another score metric to minimize the identification risk of inferring unknown attacks. To detect malicious TCP packets, Bitton and Shabtai [16] proposed a network-based intrusion detection system specifically for securing remote desktop connections. The system utilized an innovative machine learning-based anomaly detection technique for finding malicious TCP packets that carried exploits aimed at the remote desktop protocols server. High-speed networks need to process a large amount of network traffic in real time, and it is difficult to implement intrusion detection models under large amounts of big data. To process network content and build reliable machine learning-based intrusion detection models, Viegas et al. [17] proposed a new scalable and persistent intrusion detection architecture. Using deep learning and generative adversarial networks, Shu et al. [18] explored distributed SDN and designed a cooperative intrusion detection system for VANET that enabled multiple SDN controllers to jointly train a global intrusion detection model for the entire network without directly exchanging their subnetwork flows.

In fact, both communication topologies and features should be taken into account in IDD design due to the fact that the decisions made on communication features alone are not reliable. Given the difficulty of making out the specific relations between the communication topologies and the corresponding features, specific machine learning technologies, i.e., graph neural networks and deep reinforcement learning algorithms [19], should be adopted. Although machine learning technologies can efficiently detect and defend against intrusions in CPS, users might suffer from privacy leakage problems [20] due to users' data not being properly dealt with. In addition, since CPS intrusions have become more intelligent and the heterogeneity problem of CPS still exists, various domains may have specific specifications regarding the standards and objectives of security, and the IDD mechanism for one CPS domain may not match the other one.

2.3. The Proposed PIDD Framework.

The framework of PIDD is shown in Figure 2, which consists of three modules: a privacy-enhanced communication topology graph generation module, a graph convolutional network-based user evaluation module, and a deep reinforcement learning-based intruder identification and processing module.

(i) *Privacy-Enhancing Communication Topology Map Generation Module.* This module first collects each user's communication topology map and features from all border routers. Then, the privacy-enhancing communication topology graph is constructed by two variational graph autoencoders (VGAE) [21] using the intrasystem and intersystem communication topology graphs, respectively. Next, appropriate noise is injected to ensure privacy protection of user communication features.

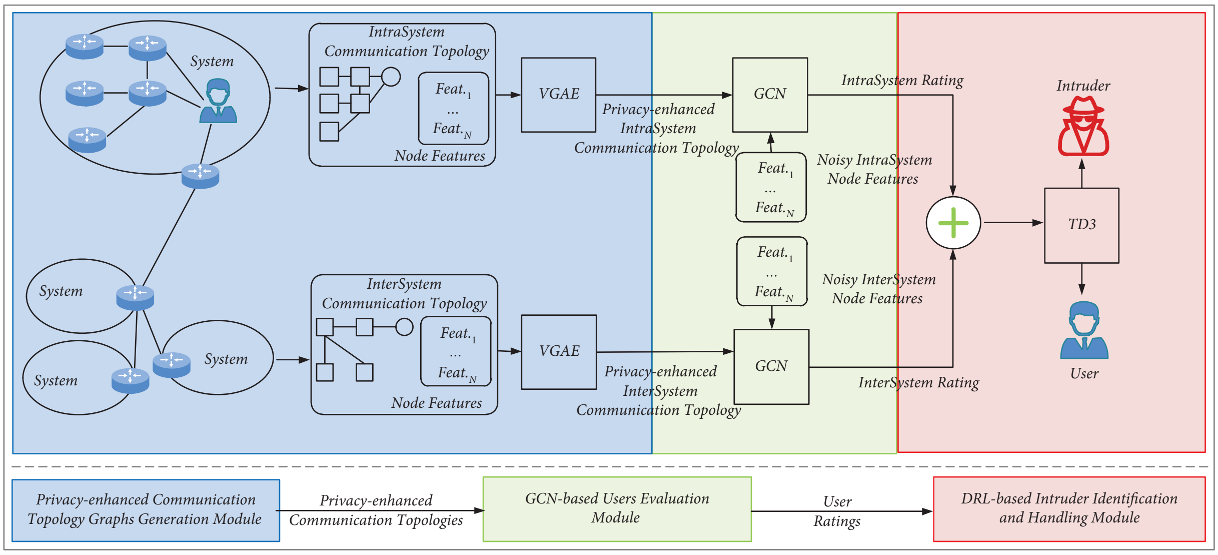

System
IntraSystem Communication Topology
Feat.$_1$
...
Feat.$_N$
Node Features
VGAE
Privacy-enhanced IntraSystem Communication Topology
GCN
IntraSystem Rating
Intruder
Noisy IntraSystem Node Features
TD3
Noisy InterSystem Node Features
User
System
System
System
InterSystem Communication Topology
VGAE
Privacy-enhanced InterSystem Communication Topology
GCN
InterSystem Rating
Privacy-enhanced Communication Topology Graphs Generation Module
Privacy-enhanced Communication Topologies
GCN-based Users Evaluation Module
User Ratings
DRL-based Intruder Identification and Handling Module

Figure 2: The framework of the proposed PIDD.

(ii) *GCN-Based User Evaluation Module*. Based on privacy-enhancing topological graphs and noisy node features, uses a graph convolutional network (GCN) [22] to evaluate users as potential regular users, intruders in the system, or intersystem intruders.

(iii) *DRL-Based Intrusion Detection and Defense Module*. This module adopts the twin delayed deep deterministic policy gradient algorithm (TD3) based on deep reinforcement learning to judge whether a user is an intruder and how to deal with different categories of users. Based on the final decision, users detected as intruders will be banned from communicating within or across systems.

In PIDD, to efficiently detect and defend intrusions, two entities of CPS, namely users and routers, are defined as follows.

(i) *Users*. There are two types of users considered in this paper. One is the normal user, while the other one is the intruder. Normal users communicate with other users within the system or cross-systems, while the intruders might launch intrusions to do different levels of damage to intrasystem routers or border routers and eventually paralyse the entire CPS.

(ii) *Routers*. For each system, there are several intrasystem routers, which coordinate the intrasystem communications, and a system border router, which is responsible for cross-system communication routing. Due to the significance of routers, to reduce the quality of service of CPS, intruders might target routers and launch the following intrusions: denial of service attacks, botnet attacks, and infiltration attacks, which are difficult to detect merely based on the features of the communication data. Within the entire CPS, the core router that coordinates all intersystems communications. We deploy the intrusion detection module on the core router to detect both intersystem intrusions and intrasystem intrusions. The intrusion detection module collects users' communication topology graphs and the corresponding features from all region-border routers for further analysis to detect intruders.

3. Models and Algorithms for the PIDD

All three modules of the proposed PIDD work collaboratively to detect and defend against intrusions in CPS, which are elaborated on in details.

3.1. Privacy-Enhanced Communication Topology Graphs Generation Module. Recall that both communication topology graphs and features of each user will be used to determine whether this user is an intruder or not. However, without proper privacy preservation, this information about users will be exposed. Injecting the proper noises can solve this problem. However, doing so will raise two other problems: (i) whether both communication topology graphs and features will be injected with noises; (ii) how much noises should be injected without causing serious detection accuracy degradation. The feasible solution to the first problem is to inject noises into communication features only. The reason for that is as follows: In order to ensure the privacy of the topology graph, the degree of each node within will be added as noise. Then, one should reconstruct the graph from the latest degree sequence. However, it is difficult due to the fact that the degree sequence might not satisfy the basic requirements of graph reconstruction [23]. Even if it is possible to reconstruct the graph, the intrusion detection accuracy will be greatly reduced, because as more communication links are added to the graph, some links will actually never exist in reality. That indicates that noise can be added to communication features only. To solve the second problem, we let each feature of the communication be normalized and added a random sampled noise from the normal distribution. Since the noise injection will result in the detection accuracy degradation, each noise is associated with a discount factor that ranges from 5% to 15%, with an increment of 5%.

We are aware that even if the communication features are protected by noise disturbance, there is always a chance that the original features will be discovered by using generative adversarial networks (GAN) [24], especially when the communication topology graphs remain the same. Thereby, we employ the VGAE to realize further privacy preservation. Basically, VGAE exploits latent variables and is able to learn interpretable latent representations for undirected graphs by using GCN as an encoder and a simple inner-product decoder. In VGAE, each communication topology graph is treated as an undirected and unweighted graph. For each graph, an adjacency matrix with diagonal elements set to 1, a degree matrix, and a random latent variable are introduced. The inference model used in VGAE is parameterized by a two-layer GCN in which both a mean vector matrix and a latent variable variance matrix are constructed. Unlike inference models, generative models are given by inner products between latent variables. VGAE takes the variational lower bound as the optimization objective of variational parameters. Note that we feed two different VGAEs with the intrasystem communication topology graphs and the intersystem communication graph of each user, respectively, to construct the individual privacy-enhanced communication topology graphs. Obviously, these two VAGEs should be trained with pairs of communication topology graphs and features of intruders or users in advance. To sum up, all VAGEs of the proposed PIDD are responsible for privacy preservation during intrusion detection.

3.2. GCN-Based Users Evaluation Module.

Once privacy-enhanced intrasystem and intersystem communication topology graphs are constructed by VGAEs, we employ two GCNs to rate the user and generate the intrasystem rating and the intersystem rating, respectively.

Specifically, there are many irregular data structures. The typical ones are graph structures or topological structures, i.e., social networks, chemical molecular structures, knowledge graphs, and communication topology graphs. Similar to CNN, GCN is a feature extractor of graph data that requires both an adjacent matrix and a feature matrix so that these features can be used to classify graph data for node classification, graph classification, edge prediction, and graph embedding. In this paper, both intrasystem and intersystem intruder identification are referred by the graph classification. That suggests we can train GCNs with the labelled pairs of privacy-enhanced communication topology graphs and noisy node features about intruders constructed by using VGAEs. Once both GCNs are well trained, the GCNs' classification results about a user are considered as the intrasystem rating and intersystem rating of that user, respectively.

3.3. DRL-Based Intruders' Identification and Handling Module.

It is worth mentioning that two ratings of the user, namely the intrasystem rating and the intersystem rating, cannot guarantee the user is an intruder. For example, even if both GCNs are well trained, there is always a chance that a normal user is misjudged as an intruder and vice versa due to the fact that the original communication topology graphs are altered by VGAEs, and the corresponding features are added with noises. Thereby, we introduce the overall rating of each user by calculating the weighted sum of two ratings. If the overall rating is higher than 0.5, then this user is a normal user; otherwise, the user is an intruder. To defend against intrusions, the intruder should be eliminated from the communication system of the CPS. However, some users might have overall ratings almost equal to 0.5, which might result from occasionally launching intrusions against routers in CPS. Thereby, for a user whose intrasystem rating is higher than 0.5, the intrasystem communication of this user should be forbidden; otherwise, the intersystem communication of this user should be banned.

Since the final decision is made based on the overall rating, the pair of weights should be calculated to improve intrusion detection accuracy. Note that each weight ranges from 0 to 1, with the sum of all weights equal to 1. That suggests the optimal pair of weights should be searched in a continuous space. As an off-policy method, DQN does not use the real action of the interaction each time it learns but uses the action that is currently considered to be the most valuable to update the objective value function, so there will be an overestimation of the Q value. Compared with DQN, TD3 uses two critical networks to estimate the action value function and uses soft update, policy noise, delayed learning, and gradient interception methods to solve the problem of overestimation. Thereby, we develop a twin delayed deep deterministic policy gradient (TD3) based intrusion detection mechanism. Specifically, the TD3 algorithm requires an actor-network π, a target actor network π', two critic networks Q_1 and Q_2, and their target network Q_1' and Q_2'. Basically, the network of participants chooses the action that should be taken for the state, and the network of critics evaluates this choice and prevents overestimation. We first give the definitions of state, action, and reward, respectively, as follows:

(i) *State*. Since each user might be a normal user or an intruder, let 0 represent the user being a normal one and 1 represent the user's being an intruder. Thereby, the state is constructed as a vector that consists of the binary representation of intrusion detection for all users.

(ii) *Action*. Recall that intrusion detection depends on the intrasystem rating and the intersystem rating of each user, both of which are coordinated by a pair of weights to generate the overall rating. Therefore, the pair of weights serves as the action. As the sum of two weights is equal to 1, if either weight is higher than 0.5, then the corresponding intrusion detection result is more dominant than the other. Moreover, the action should include countermeasures against intruders. If the user is an intrasystem intruder, an intersystem intruder, or both, then the user is forbidden to communicate with intrasystem users, intersystem users, or both accordingly.

(iii) *Reward*. The goal of intrusion detection is to detect and eliminate intruders to greatly reduce the number of intrusions in CPS. That suggests the intrusions prevented should be taken into account in the reward calculation. Moreover, the communication traffic should be considered as well, asimproperly chosen weights might result in a significant communication traffic drop. Thereby, we let the normal communication traffic, which equals the overall communication traffic minus the intrusion traffic, be the reward to evaluate the performance of the proposed PIDD.

In TD3 training, we randomly sample N experience to update the critic network with the loss function,

$$L\left(\vartheta^{Q_i}\right) = \frac{1}{N}\sum_{j}^{N}\left[Q_i\left(s_j, a_j|\vartheta^{Q_i}\right) - Y_j\right]^2, \tag{1}$$

where

$$Y_j = r_j + \gamma\left[Q_i'\left(s_{i+1}, \pi\left(s_{i+1}|\vartheta^{\pi'}\right)|\vartheta^{Q_i'}\right)\right]_{i=1,2}. \tag{2}$$

Thereby, we have,

$$\vartheta^{Q_i} \leftarrow \vartheta^{Q_i} - \eta\frac{\partial L\left(\vartheta^{Q_i}\right)}{\partial\vartheta^{Q_i}}. \tag{3}$$

Then, we update the actor-network π by optimizing the objective function,

$$J\left(\vartheta^{\pi}\right) = \sum_{j}^{N}\left[Q_1\left(s, a|\vartheta^{Q_1}\right)\pi\left(s_j|\vartheta^{\pi}\right)|s = s_j, a = \pi\left(s_j|\vartheta^{\pi}\right)\right]. \tag{4}$$

with

$$\vartheta^{\pi} \leftarrow \vartheta^{\pi} + \iota\frac{\partial J\left(\vartheta^{\pi}\right)}{\partial\vartheta^{\pi}}. \tag{5}$$

Next, the parameters of target networks $\vartheta^{Q'}$ and $\vartheta^{\pi'}$ are updated with a learning rate κ.

Note that the training process for all three modules of the proposed PIDD is as follows. First, VGAE and GCN are trained using all labelled communication topology maps and features of users and intruders in the privacy-enhancing communication topology map generation module and the GCN-based user evaluation module. Then, TD3 is trained using the corresponding ratings in the DRL-based intruder identification and a processing module. Once trained, the proposed PIDD is able to determine whether a user is an intruder based on the user's communication topology and characteristics.

The main symbols and their meanings for the proposed PIDD are shown in Table 1.

Table 1: Main symbols and meanings.

Symbol	Meaning
CPS	Cyber-physical systems
IDD	Intrusion detection and defense
GCN	Graph convolutional network
VGAE	Variational graph autoencoders
TD3	Twin delayed deep deterministic policy gradient
π	Actor network
π'	Target actor network
$Q_{i=1,2}$	Critic network
$Q'_{i=1,2}$	Target critic network
η, ι, κ	Learning rate

4. Numerical Results

To evaluate the performance of the proposed mechanism, we target three attacks, namely the denial of service attack (DoS), the botnet attack (Bot), and the infiltration attack (Inf), to prevent intrusion. The experiment was conducted to evaluate the performance of the proposed PIDD in Python on a computer equipped with an i7 6.4GHZ processor, 32G memory, and a win7 64-bit system. In VGAE, initialized weights are set as described in [21], and a 32-dim hidden layer and 16-dim latent variables are used in all experiments. There are up to 200 iterations of training using Adam with a learning rate of 0.01.

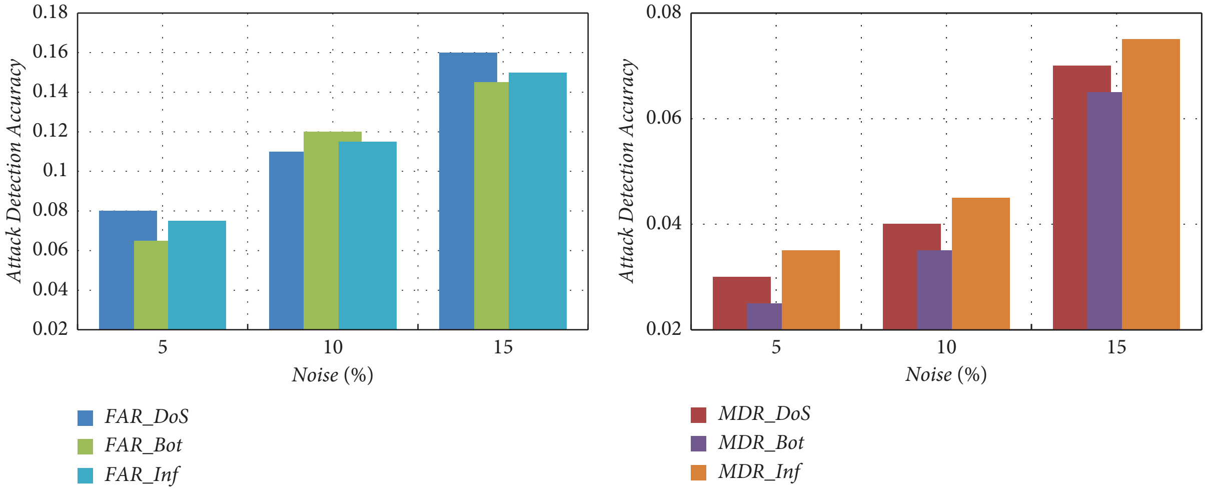
The "CSE-CIC-IDS2018" dataset, which is available at "https://www.unb.ca/cic/datasets/ids-2018.html," is used in this experiment. The dataset includes seven different attack scenarios: Brute-force, Heartbleed, Botnet, DoS, DDoS, Web attacks, and infiltration of the network from inside. The attacking infrastructure includes 50 machines, and the victim organization has 5 departments and includes 420 machines and 30 servers. The dataset includes the captured network traffic and system logs of each machine, along with 80 features extracted from the captured traffic by using CICFlowMeter-V3. To facilitate the performance evaluation, each cyber-physical system contains at most 16 routers and 1 border router. Both intrasystem communication topology graphs and intersystem communication topology graphs are extracted first. Then, all these topology graphs and communication features are used to determine whether users are intruders. The following indexes are employed to evaluate the performance of the PIDD with the consideration of different percentages of noise added.

(i) *Detection Accuracy*. Both the false alarm rate (FAR) and the miss detection rate (MDR) are applied to evaluate the detection accuracy.

(ii) *Intrusion Prevention Percentage*. The percentage of intrusions prevented in overall intrusions launched

(iii) *Privacy Preservation Percentage*. The differences between the original communication topology graphs and the privacy-enhanced ones are measured in the privacy preservation percentage.

Figure 3 shows the detection accuracy of adding different percentages of noise. As shown in Figure 3, we find that the FAR and MDR of all three types of intrusions increase as the



(a)

(b)

Figure 3: Detection accuracy with different percentages of noise added. (a) FAR and (b) MDR.

percentage of added noise increases. Furthermore, PIDD achieves on average 6%, 11.5%, and 14% of FAR and 3%, 4%, and 7% of MDR, and all noises are 5%, 10%, and 15% intrusion, respectively. What's more, even though the features add up to 15% noise, the highest FAR and MDR of PIDD are still lower than 16% and 8%. This is because the proposed PIDD combines the graph variational autoencoder and the graph neural network and considers intrasystem and intersystem communication at the same time, so it can effectively discover the intrusion behavior of the attacker. Experimental results show that PIDD can accurately detect routing intrusions in CPS with noisy communication data.

Table 2 gives the intrusion prevention that adds different percentages of noise in terms of intrasystem intrusion and intersystem intrusion. As observed in Table 2, it is clear that the percentage of intrusion prevention decreases with the percentage of added noise, as expected. Note that PIDD is more effective at preventing intrasystem intrusion than intersystem intrusion. This may be due to intruders launching intrasystem intrusions more frequently, making intrusion patterns harder to learn. Additionally, PIDD can detect and block at least 83% of intrasystem intrusions and 81% of intersystem intrusions, even when up to 15% of the noise is added to the communication signature. The intrusion prevention shown in Table 2 shows that PIDD can effectively defend against routing intrusion in CPS because the variational graph autoencoder and graph neural network adopted by PIDD can well capture the characteristics of intrusion behavior.

Table 2: Intrusion prevention with different percentages of noise added.

Intrusion	Noise		
	5 (%)	10 (%)	15 (%)
Intra_DoS	93	87	83
Inter_DoS	91	85	82
Intra_Bot	93	87	83
Inter_Bot	89	85	84
Intra_Inf	92	87	83
Inter_Inf	88	86	81

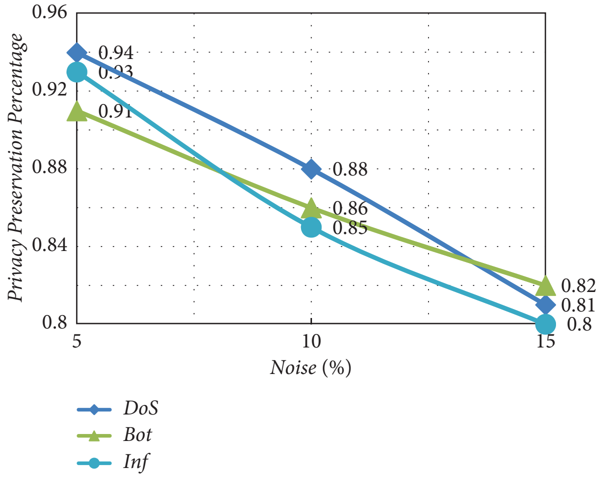


Figure 4: Privacy preservation with different percentages of noise added.

Figure 4 shows the privacy protection of adding different percentages of noise. It is worth mentioning that, in order to protect the privacy of users, only noise has been added to the communication function. As the percentage of added Gaussian noise increases, the user's privacy is better protected. On the other hand, VGAE modifies the user's communication topology map to a privacy-enhanced communication topology map as the input to the GCN-based classifier. Both noise injection and VGAE-based graph modification provide user privacy protection, which is verified in this figure. Furthermore, PIDD achieves on average about 91%, 86%, and 82% privacy preservation, adding 5%, 10%, and 15% of noise, respectively. This shows that PIDD can protect the privacy of users during the intrusion detection process.

5. Conclusion

In order to improve the efficiency and accuracy of intrusion detection and protect user privacy from being leaked during the CPS intrusion detection process, this paper proposes a privacy-enhanced intrusion detection and defense mechanism based on deep reinforcement learning. Specifically, first, two variational graph autoencoders are trained to generate privacy-enhanced communication topology graphs. Second, two graph convolutional networks are trained based on the privacy-enhanced communication topology map and noise features to perform user evaluation. Finally, a deep reinforcement learning algorithm TD3 is applied to identify intruders and execute appropriate countermeasures. We conducted validation experiments on the “CSE-CIC-IDS2018” dataset. Experimental results show that the proposed PIDD achieves excellent performance in terms of intrusion detection accuracy, intrusion prevention percentage, and privacy protection.

Although the proposed algorithm can perform intrusion detection under the condition of preserving privacy, the detection accuracy needs to be improved. Our future research directions include how to further combine the characteristics of intrusion behavior with the communication topology of intrusion.

Data Availability

The “CSE-CIC-IDS2018” dataset, which is available at “https://www.unb.ca/cic/datasets/ids-2018.html,” is used in this experiment. We have given this site in our manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Nature Science Foundation of China (Grant numbers: 61902167, 32201679), the Science Foundation of the Fujian Province, China (Grant numbers: 2021J011015, 2022J05230), and Foundation of Fuzhou Institute of Oceanography (Grant number: 2022F07).

References

[1] S. Singh, N. Yadav, and P. K. Chuarasia, “A review on cyber physical system Attacks: issues and challenges,” in *Proceedings of the 2020 International Conference on Communication and Signal Processing (ICCSP)*, pp. 1133–1138, IEEE, Chennai, India, July 2020.

[2] P. Freitas de Araujo-Filho, G. Kaddoum, D. R. Campelo, A. Gondim Santos, D. Macedo, and C. Zanchettin, “Intrusion detection for cyber–physical systems using generative adversarial networks in fog environment,” *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6247–6256, 2021.

[3] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, “DeepFed: federated deep learning for intrusion detection in industrial cyber–physical systems,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5615–5624, 2021.

[4] S. E. Quincozes, D. Mossé, D. Passos, C. Albuquerque, L. S. Ochi, and V. F. dos Santos, “On the performance of GRASP-based feature selection for CPS intrusion detection,” *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 614–626, 2022.

[5] Z. Huang, Y. Wu, N. Tempini, H. Lin, and H. Yin, “An energy-efficient and trustworthy unsupervised anomaly detection framework (EATU) for IIoT,” *ACM Transactions on Sensor Networks*, 2022.

[6] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, “A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks,” *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9463–9472, 2021.

[7] Y. Xie, D. Feng, Y. Hu, Y. Li, S. Sample, and D. L. Long, “Pagoda: a hybrid approach to enable efficient real-time provenance based intrusion detection in big data environments,” *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1283–1296, 2020.

[8] H. Liu, S. Zhang, P. Zhang et al., “Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6073–6084, 2021.

[9] L. Qi, Y. Yang, X. Zhou, W. Rafique, and J. Ma, “Fast anomaly identification based on multiaspect data streams for intelligent intrusion detection toward secure industry 4.0,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6503–6511, 2022.

[10] X. Wang, S. Garg, H. Lin et al., “Towards accurate anomaly detection in industrial internet-of-things using hierarchical federated learning,” *IEEE Internet of Things Journal*, vol. 9, no. 10, 2022.

[11] Q. Cui, Z. Zhu, W. Ni, X. Tao, and P. Zhang, “Edge-intelligence-empowered, unified authentication and trust evaluation for heterogeneous beyond 5G systems,” *IEEE Wireless Communications*, vol. 28, no. 2, pp. 78–85, 2021.

[12] C. Shen, C. Liu, H. Tan, Z. Wang, D. Xu, and X. Su, “Hybrid-augmented device fingerprinting for intrusion detection in industrial control system networks,” *IEEE Wireless Communications*, vol. 25, no. 6, pp. 26–31, 2018.

[13] T. Yu and X. Wang, “Topology verification enabled intrusion detection for in-vehicle CAN-FD networks,” *IEEE Communications Letters*, vol. 24, no. 1, pp. 227–230, 2020.

[14] L. Yang, A. Moubayed, and A. Shami, “MTH-IDS: a multi-tiered hybrid intrusion detection system for Internet of vehicles,” *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 616–632, 2022.

[15] J. Yang, X. Chen, S. Chen, X. Jiang, and X. Tan, “Conditional variational auto-encoder and extreme value theory aided two-stage learning approach for intelligent fine-grained known/unknown intrusion detection,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3538–3553, 2021.

[16] R. Bitton and A. Shabtai, “A machine learning-based intrusion detection system for securing remote desktop connections to electronic flight bag servers,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1164–1181, 2021.

[17] E. Viegas, A. O. Santin, and V. Abreu Jr, “Machine learning intrusion detection in big data era: a multi-objective approach for longer model lifespans,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 366–376, 2021.

[18] J. Shu, L. Zhou, W. Zhang, X. Du, and M. Guizani, “Collaborative intrusion detection for VANETs: a deep learning-based distributed SDN approach,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4519–4530, 2021.

[19] Z. Yan, J. Ge, Y. Wu, L. Li, and T. Li, “Automatic virtual network embedding: a deep reinforcement learning approach with graph convolutional networks,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1040–1057, 2020.

[20] Y. Wu, H.-N. Dai, H. Wang, and K.-K. R. Choo, “Blockchain-based privacy preservation for 5G-enabled drone communications,” *IEEE Network*, vol. 35, no. 1, pp. 50–56, 2021.

[21] T. N. Kipf and M. Welling, “Variational Graph Auto-Encoders,” November 2016, https://arxiv.org/abs/1611.07308.

[22] T. N. Kipf and M. Welling, “Semi-supervised Classification with Graph Convolutional Networks,” September 2016, https://arxiv.org/abs/1609.02907.

[23] H. Huang, D. Zhang, F. Xiao, K. Wang, J. Gu, and R. Wang, “Privacy-preserving approach PBCN in social network with differential privacy,” *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 931–945, 2020.

[24] C. Xu, J. Ren, D. Zhang, Y. Zhang, Z. Qin, and K. Ren, “GANobfuscator: mitigating information leakage under GAN via differential privacy,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2358–2371, 2019.