International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I5P209

Volume 70 Issue 5, 74-79, May 2022

Original Article

Improvement of Wireless Sensor Networks Against Service Attacks Based on Machine Learning

Gang Xu[1], Allemar Jhone P. Delima[2], Ivy Kim D. Machica[3], Jan Carlo T. Arroyo[4], Zhengfang He[5], Weibin Su[6]

[1,3,5,6]*College of Information and Computing, University of Southeastern Philippines, Davao City, Davao del Sur, Philippines*
[1,5,6]*Edge Computing Network Center, Yunnan Technology and Business University, Kunming, China*
[2,4]*Institute of Information and Computer Studies, Northern Iloilo State University, Iloilo, Philippines*
[4]*College of Computing Education, University of Mindanao, Davao City, Davao del Sur, Philippines*

[1]480580@qq.com

Received: 02 February 2022 Revised: 16 April 2022 Accepted: 03 May 2022 Published: 19 May 2022

Abstract *- With the rapid development of sensor technology, wireless sensor networks (WSNs) composed of a large number of low-cost, high-performance and plug and play sensor nodes have occupied more and more application scenarios in society, such as medical and health, environmental monitoring, business activities, and national defense security. However, a WSN is a distributed network exposed in an open environment. Each node is independent of the other, and the lack of a central node and monitoring node makes it vulnerable to malicious attacks, and it is difficult to prevent. Denial of Service (DoS) attack is one of them. Support Vector Machine (SVM) and K-Nearest Neighbor (KNN) algorithms prevent network attacks, but these methods have specific disadvantages such as low quality, complex time, and data loss. This paper proposes a method using Random Support Vector Regression (RSVC) to improve the quality of preventing distributed denial of service (DDoS) attacks in WSN. It provides the results of various simulation scenarios and compares the corresponding data. The research on DDoS prevention is very helpful in understanding the anti-attack performance of wireless sensor network nodes. The impact of DoS attacks on wireless sensor networks' performance is considered the key research of these problems.*

Keywords *- Machine learning, random support vector regression (RSVR), support vector machine (SVM), wireless sensor network (WSN).*

1. Introduction

Many experts have long discussed the application of wireless sensor networks. Wireless sensor networks are widely used in medical and health, environmental monitoring, commercial activities, and national defense security, such as logistics scheduling, military investigation, hydrological observation, positioning, and tracking. These applications include multiple levels of monitoring and control. By deploying many low-cost, high-performance and plug and play micro sensor nodes, data collection can be realized in some key areas. in military applications, real-time information on the battlefield is obtained, and field information is collected and analyzed by various special sensors. in medical applications, it is used for patient discovery and examination. These nodes transmit data through wireless networks, but due to the limitations of energy, computing, storage, and other resources, they can not guarantee and provide good security, so wireless sensor networks face great challenges. There are many kinds of attacks on wireless sensor networks. DDoS is a common and effective one. There are not many security methods in the existing research. Therefore, this paper designs a lightweight security method to deal with DDoS attacks effectively.

A WSN consists of many cheap micro sensor nodes deployed in a specific monitoring area, a multi-hop ad hoc network that communicates wirelessly. Its purpose is to perceive, collect or process the information of a perceived object in the network coverage area through the cooperation of each node, and send it to the observer. The sensor node comprises the sensor, data processing, communication, and energy supply modules with multiple built-in sensors. It can control the surrounding environment's temperature, humidity, noise, pressure, and gas composition. It can measure the size, direction, speed, and other physical quantities of the moving object. Node data is transmitted to base stations and user terminals through multi-hop wireless routing using wireless network technology.

In most cases, open wireless networks are used to transmit sensitive information. Due to the characteristics of nodes, the limitations of resources such as the battery, processing capacity, and storage are present in wireless networking architecture. Similar to traditional wireless networks, WSN also faces severe security challenges. on the one hand, WSN uses open communication media and may be deployed in an unattended environment, making the

operating network vulnerable to various attacks and even node data theft. on the other hand, due to the limited node resources in WSN, the security mechanisms in traditional wireless networks are often not suitable for WSN. Therefore, how to effectively deal with various possible attacks in WSN has become a hot and difficult point in the current WSN research field. This paper focuses on preventing DDoS, a common and effective attack means.

DOS attack means that an attacker hijacks a node in the network and sends a large amount of spam. Its purpose is to weaken the ability of wireless sensor networks to provide services and deplete the energy of sensor nodes and lead to the death of nodes to destroy and subvert the whole network. DOS attacks may occur in all four layers of the network structure of WSN. Distributed denial of service (DDoS) attack is one of the most well-known attacks. It is a special form of denial-of-service attack based on DOS. It is a distributed and coordinated large-scale attack. DDoS may occur in all layers of the WSN network structure. This paper will use the machine learning method to provide solutions in the network layer of wireless sensor networks.

2. Literature Review

The literature on denial of service attacks is not new. However, each type of attack has a slightly different concept [1]. Some researchers have summarized the clear characteristics of DDoS attacks given by the reference model of Internet Protocol (IP) from the perspective of Open Systems Interconnection (OSI) or transmission control protocol (TCP) denial [2]. Others refused to assist in the attack and tried to use other display devices to focus on positioning and mitigation strategies [3]. DDoS is one of the challenging projects in the current security research. Many researchers try to improve the defense effect of this attack by means of machine learning. Sunil ghildiyal et al. described the types of DoS attacks [4]. Ahmad et al. used feature selection and clustering methods to improve the node life cycle [5], and Premkumar et al. proposed a deep learning algorithm to detect DoS attacks [6].

Moreover, Al-Issa et al. compared two machine learning algorithms to detect attacks on specific data sets [7]. Heng Zhang et al. conducted theoretical research on a networked control system plan [8]. These studies can effectively deal with DOS attacks in specific environments, but there are few schemes for DDoS. This paper proposes to use SVM and KNN to improve the detection and defense of DoS attacks.

Although there are limited articles on DDoS attacks, many authors admit that DDoS attacks are the association and service system modeling systematically displayed on remote sensor organizations [9]. Arranging all current technologies as a series of prerequisites will allow a careful and itemized investigation of the proposed strategy according to common sense and Implementation in any case [10], [11]. The demonstration is regarded as an important, useful, and powerful system that should have certain characteristics [12]. Different techniques can be used to process and evaluate those that need to consider selected attributes [13], [14].

For example, it is necessary to screen key offices, power structures, water supply, transportation organizations, media communication frameworks, agricultural enterprises, military orders, and social utilities. For example, the remote sensor organization has remote sensing network inspection and different applications for patients. Medical clinics, families, and the elderly pay attention to other physiological factors in clinical and medical care [15]. Similarly, wireless sensor networks can also identify floods, power outages, fires, storms, volcanic eruptions, or earthquakes during catastrophic events [16]- [18]. Due to DDoS attacks, portable sensors have become a necessary scenario, and their consistency is still a great danger. The attacks carried out are by no means undeniable [19]. However, attacking wireless sensor networks is a good strategy. The DDoS attack is regarded as a computerized combat program.

in addition, DDoS attacks can be carried out by an ideal staff member, enabling them to counterattack in both wired and remote organizations [20]. Artificial reasoning introduces machine learning conventions, and remote sensor organizations can obtain incredible returns from multifunctional innovation [21]. in the past decade, remote sensor networks have witnessed a progressive and thorough choice, advanced artificial reasoning innovation [22]. The focus is on organic incentive strategies, such as neural organization (in the era of neural networks), fuzzy framework, and artificial consciousness transformation tools. Its purpose is to detect a new artificial intelligence-based DDoS attack detection system based on a wireless sensor connection [23]-[26].

3. Methodology

Support Vector Machine (SVM) is proposed for binary classification, and Support Vector Regression (SVR) is an important application branch of SVM. The difference between SVM and SVR classification is that there is only one kind of sample point in SVR. The optimal hyperplane it seeks is not the most open of two or more kinds of sample points but the minimum total deviation of all sample points from the hyperplane. Random Support Vector Regression (RSVR) attack probability recognition is a statistical learning method based on RSVR classification technology. It gives a data set of learning machine input training for various reasons, such as classification, stratification, form perception, etc. Binary tag data indicates that the probability of training data being attacked is very low or high. The biggest separation of learning machine work is to find two boundary planes and separate L or -1 (attack probability) and H or +1 (high attack probability).

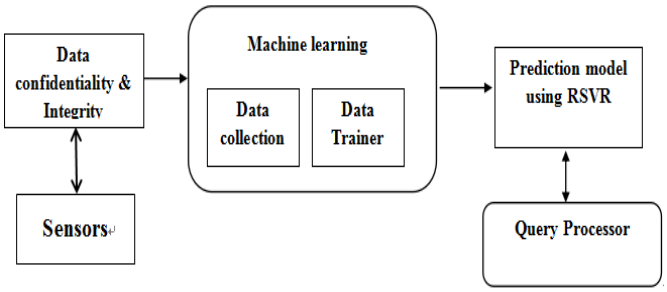

Fig. 1 Block diagram

Fig. 1 shows the Wireless Sensor Network (WSN) composed of distributed deployed small battery-based autonomous devices processed with RSVR, which monitors the environment and obtains physical data. Routers or gateways connect to deployment nodes to support many real-time applications. Because of open access, there are security problems in wireless sensor networks. in this case, external users can view by ensuring that authentication is required. in real-time applications, to achieve secure communication, they do not use many lightweight authentication mechanisms [27].

3.1. Data Confidentiality and Integrity

Sensor nodes use the open wireless network to transmit data. The confidentiality of data ensures the security of transmitting data to the network, not to mention that sensor nodes can send messages through hidden and unauthorized confidential data nodes. Encrypting data to display its content messages can prevent attacks anywhere. The data receiver shall not suddenly change or send data in the road data integrity guarantee. However, the reliability of transmitted data supports the confidentiality of data, making it more average than reliable. Malicious nodes may misunderstand or respond to sensor network messages. The best way to ensure data integrity is through sensor networks using authentication protocols. However, public-key encryption supports data integrity, and sensor networks may be incompatible due to their high cost and storage space requirements. The lightweight authentication system using symmetric key encryption is more suitable. No matter which form of authentication is adopted, it will increase the network burden and challenge the already scarce WSN network resources.

3.2. Random Support Vector Regression Dataset of Selected Attacks

The working process of RSVR is shown in Fig. 2. Here, the collection of data sets is an important process. First, there is a need to obtain a massive number of sample data for training. These datasets need to include a specific application scenario, or more application scenario data, and data sets used by different attributes in different fields. Users realize that the RSVR parameter is a key problem when selecting the appropriate kernel function to study the dataset's attributes. RSVR behavior is a feature used in various core functions of related datasets [28].

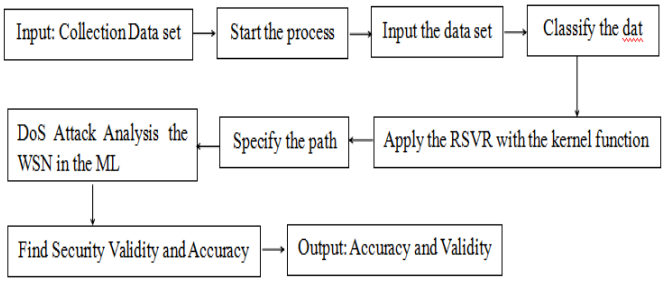

Fig. 2 Work process of RSVR

3.3. DoS Attack on Quality Protection

To prevent DoS attacks, the real hardware security index is instrumental in preparing the WSN model for discussion, and several complete versions of the project modeling language are designed [29]. in the form of noise, conflict, or attack environment, this may interfere with devices, which may accidentally interfere with wireless transactions and lead to denial-of-service attacks. Certain attacks achieve specific goals, such as network access, network infrastructure, and server applications. The affected nodes must make aggressive attempts to exhaust the available resources of additional adverse data. Therefore, users should be prevented from accessing the service. Denial of service attack refers to the enemy's ability to destroy or reduce network service arrangements. Denial of service attacks is created in different layers. in the network layer, the corpse dumping attack is easy to synchronize with the DS attack. Similar node subversion, false routing, black hole attacks, wormhole attacks, sinkhole attacks, flood attacks, and Sybil attacks [30].

4. Results and Discussion

The purpose of the simulation is to track the origin of wireless networks. The background environment adopted is NS-2, an object using command language tools. Run all network simulations using the proposed model, and then create all code and scripts.

Table 1. Simulation parameters

Parameters	Value
Simulation Tool	Ns2
Data size	100MB
Transferring Data	100
Network	Wireless Sensor Network

In Table I above, the data received from the wireless sensor network has obvious defects. Comprehensively process the data in a complex environment. Each environment has a lot of reading time. Data analysis shows that the traffic is consumed.

4.1. Analysis of Failure Measurement

Idleness refers to the arrival and cycle of data. This type of data may be caused by delay time (also known as network failure time), which occurs during node processing; that is, the interval between past bits is the smallest. Average data sends raw node data to the toolbar using average time, amount of data, and default nodes. The process of discovering the transmission time in the interface path involves a path redirection delay and buffers delay.

Table 2. Failure measure performance

No. of. data	SVM in sec	KNN in sec	RSVR in sec
10	0.5	0.8	0.9
20	0.9	1.5	2.1
30	1.6	2.5	2.9
40	2.8	3.2	3.7
50	4.4	5.3	4.8

Table II shows the process's failure performance analysis to the delay and buffers delay performance.

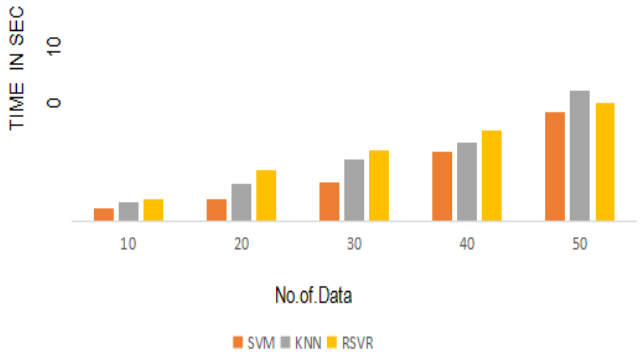

Fig. 3 Performance of packet delivery delay

Fig. 3 shows the transmission of data packet delay performance. SVM obtained 4.4%, while the KNN has 5.3%, and a 4.8% delay rate for RSVR is identified.

4.2. Secure Performance Ratio

Safety performance packet transmission rate is the ratio between the transmission sequence numbers of the transmitted data. Ensures a high rate of data transmission on the fixed link. The high packet transfer rate is specified through the holes.

Table 3. Security performance

No. of data	Security performance in (%)		
	SVM	KNN	RSVR
10	35	40	53
20	45	65	75
30	60	72	85
40	75	79	88
50	82	87	91

Table III shows the security performance using the three algorithms. Fig. 4 shows the graphical representation of the data security performance. Results show that the SVM obtained 82% accuracy over 87% accuracy using KNN and 91% using RSVR.

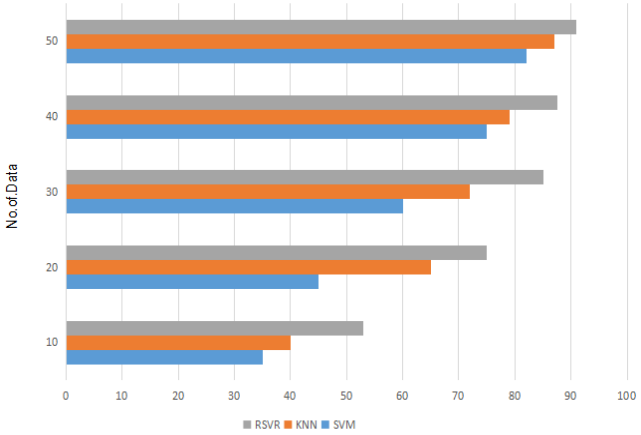

Fig. 4 Algorithm performance

4.3. Time Complexity

Simulation results show that RSVR has a reduced time over KNN and SVM. Table IV shows the indexed data for time complexity.

Table 4. Time complexity

No of data	SVM in sec	KNN in sec	RSVR in sec
10	15	12	10
20	25	22	20
30	30	28	25
40	40	32	25
50	35	30	28
60	55	45	30

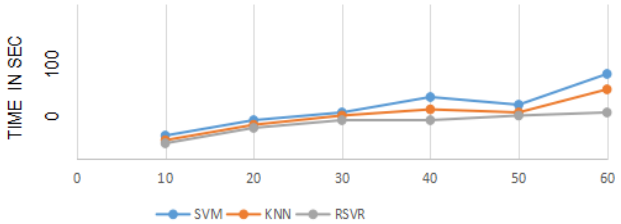

Fig. 5 Graphical representation for time complexity

Fig. 5 shows the time limits Analysis. The delay performance data count is calculated based on time. The SVM calculates a 100MB table of data transfer longer in terms of data size and complex time. The minimum amount of data sent through KNN is 45 seconds, while SVM is 55 seconds, and RSVR is 30 seconds. A reduced complex time is using the RSVR.

5. Conclusion

Wireless Sensor Network is a developing technology. With the popularization and application of artificial intelligence, it will gradually enter all aspects of human life and work. Still, it is because of its openness that it is vulnerable to various security attacks. A DDoS attack is the most common denial of service (DOS) attack. For DoS

attacks, there is much literature on famous countermeasures and defense mechanisms. At the same time, it also provides the solutions of sensor nodes for most DoS attacks, but the solutions are too complex, especially the lightweight solutions for DDoS. DDoS attacks will prevent network availability, packet retrieval, or transmission. This machine learning technology is the most efficient lightweight solution for DDoS in wireless sensor networks. RSVR attack detection technology can detect the accuracy of machine learning and defend against DoS attacks on WSNs. The algorithm proposed in this study may have limited performance in some specific environments. For future works, it is suggested to design an updated machine learning algorithm to solve the universality of DDoS detection in WSN networks.

REFERENCES

[1] D. Kim and S. An, PKC-Based DoS Attacks-Resistant Scheme in Wireless Sensor Networks, in IEEE Sensors Journal, 16(8) (2016) 2217-2218. doi: 10.1109/JSEN.2016.2519539.

[2] J. Wu, K. Ota, M. Dong, and C. Li, A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities, in IEEE Access, 4 (2016) 416-424. doi: 10.1109/ACCESS.2016.2517321.

[3] L. Shi, Q. Liu, J. Shao, and Y. Cheng, Distributed Localization in Wireless Sensor Networks Under Denial-of-Service Attacks, in IEEE Control Systems Letters, 5(2) (2021) 493-498. doi: 10.1109/LCSYS.2020.3003789.

[4] Ghildiyal S, Mishra A K, Gupta A, et al. Analysis of denial of service (dos) attacks in wireless sensor networks[J]. IJRET: International Journal of Research in Engineering and Technology, 3 (2014) 2319-1163.

[5] Ahmad R, Wazirali R, Bsoul Q, et al. Feature-selection and mutual-clustering approaches to improve dos detection and maintain wsns' lifetime[J]. Sensors, 21(14) (2021) 4821.

[6] Premkumar M, Sundararajan T V P. DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks[J]. Microprocessors and Microsystems, 79 (2020) 103278.

[7] Al-Issa A I, Al-Akhras M, ALsahli M S, et al. Using machine learning to detect DoS attacks in wireless sensor networks[C]//2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). IEEE, (2019) 107-112.

[8] Y. Kirsal Ever, Secure-Anonymous User Authentication Scheme for e-Healthcare Application Using Wireless Medical Sensor Networks, in IEEE Systems Journal, 13(1) (2019) 456-467.doi: 10.1109/JSYST.2018.2866067.

[9] C. Pu and S. Lim, A Lightweight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation, in IEEE Systems Journal, 12(1) (2018) 834-842. doi: 10.1109/JSYST.2016.2535730.

[10] C. Hongsong, M. Caixia, F. Zhongchuan, and C. Lee, Novel LDoS attack detection by Spark-assisted correlation analysis approach in wireless sensor network, in IET Information Security, 14(4) (2020) 452-458. doi: 10.1049/iet-ifs.2018.5512.

[11] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, Data Collection for Security Measurement in Wireless Sensor Networks: A Survey, in IEEE Internet of Things Journal, 6(2) (2019) 2205-2224. doi: 10.1109/JIOT.2018.2883403.

[12] O. A. Osanaiye, A. S. Alfa and G. P. Hancke, Denial of Service Defence for Resource Availability in Wireless Sensor Networks, in IEEE Access, 6 (2018) 6975-7004. doi: 10.1109/ACCESS.2018.2793841.

[13] H. Chen, C. Meng, Z. Shan, Z. Fu, and B. K. Bhargava, A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation, in IEEE Access, 7 (2019) 32853-32866. doi: 10.1109/ACCESS.2019.2903816.

[14] A. Tsiota, D. Xenakis, N. Passas and L. Merakos, on Jamming and Black Hole Attacks in Heterogeneous Wireless Networks, in IEEE Transactions on Vehicular Technology, 68(11) (2019) 10761-10774. doi: 10.1109/TVT.2019.2938405.

[15] C. Lyu, X. Zhang, Z. Liu, and C. Chi, Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things Against DoS Attacks, in IEEE Access, 7 (2019) 31068-31082. doi: 10.1109/ACCESS.2019.2902843.

[16] Dr.G.Kavithaa, M.Prithivi Raj, 2019, Dynamic Signal Driving Strategy Based High Speed and Low Powered Dual Edge Triggered Flip Flop Design Used Memory Applications, in Microprocessors and Microsystems, Elsevier, 71 (2019) . Https://Doi.Org/10.1016/J.Micpro.2019.102879.

[17] J. Padmanabhan and V. Manickavasagam, Scalable and Distributed Detection Analysis on Wormhole Links in Wireless Sensor Networks For Networked Systems, in IEEE Access, 6 (2018) 1753-1763. Doi: 10.1109/ACCESS.2017.2780188.

[18] H. Zhang, P. Cheng, L. Shi, and J. Chen, Optimal Dos Attack Scheduling in Wireless Networked Control System, in IEEE Transactions on Control Systems Technology, 24(3) (2016) 843-852.Doi: 10.1109/TCST.2015.2462741.

[19] R. Huang, L. Ma, G. Zhai, J. He, X. Chu, and H. Yan, Resilient Routing Mechanism For Wireless Sensor Networks With Deep Learning Link Reliability Prediction, in IEEE Access, 8 (2020) 64857-64872. Doi: 10.1109/ACCESS.2020.2984593.

[20] F. Afianti, Wirawan, and T. Suryani, Lightweight and Dos Resistant Multiuser Authentication in Wireless Sensor Networks For Smart Grid Environments, in IEEE Access, 7 (2019) 67107-67122. Doi: 10.1109/ACCESS.2019.2918199.

[21] A.Sangeetha, Dr.M.Chandrasekaran, Dr.G.Kavithaa, 2020, Time Situate Recurrence Estimation Technique For Efficient Data Collection in War Field Sensor Network, in Microprocessors and Microsystems, Elsevier, 73 (2020). Https://Doi.Org/10.1016/J.Micpro.2020.102988.

[22] Yu, D., Kang, J., & Dong, J., Service Attack Improvement in Wireless Sensor Network Based on Machine Learning. Microprocessors and Microsystems, 80 (2021) 103637.

[23] Kavousi-Fard A, Su W, Jin T. A Machine-Learning-Based Cyber-Attack Detection Model For Wireless Sensor Networks in Microgrids[J]. IEEE Transactions on Industrial Informatics, 17(1) (2020) 650-658.

[24] Khan ZA, Samad A. A Study of Machine Learning in Wireless Sensor Networks [J]. Int. J. Comput. Netw. Appl, 4(4) (2017) 105-112.

[25] Khattab A, Youssry N. Machine Learning For Iot Systems[J]. Internet of Things (Iot), (2020) 105-127.

[26] Mamdouh M, Elrukhsi M A I, Khattab A. Securing The Internet of Things and Wireless Sensor Networks Via Machine Learning: A Survey[C]//2018 International Conference on Computer and Applications (ICCA). IEEE, (2018) 215-218.

[27] G Martín A, Fernández-Isabel A, Martín De Diego I, Et Al. A Survey For User Behavior Analysis Based on Machine Learning Techniques: Current Models and Applications[J]. Applied Intelligence, 51(8) (2021) 6029-6055.

[28] Singh G, Khare N. A Survey of Intrusion Detection From The Perspective of Intrusion Datasets and Machine Learning Techniques[J]. International Journal of Computers and Applications, (2021) 1-11.

[29] Alloghani M, Al-Jumeily D, Hussain A, Et Al. Implementation of Machine Learning and Data Mining to Improve Cybersecurity and Limit Vulnerabilities to Cyber Attacks[M]//Nature-Inspired Computation in Data Mining and Machine Learning. Springer, Cham, (2020) 47-76.

[30] Ahmad R, Wazirali R, Bsoul Q, Et Al. Feature-Selection and Mutual-Clustering Approaches to Improve Dos Detection and Maintain Wsns' Lifetime[J]. Sensors, 21(14) (2021) 4821.