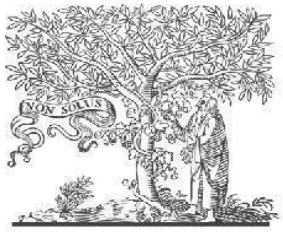
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 6th July 2024. Link

https://ijiemr.org/downloads.php?vol=Volume-13& issue=issue07

DOI: 10.48047/IJIEMR/V13/ISSUE 07/3

Title Probabilistic Evaluation of a Wireless Sensor Network (WSN) Ensemble Attacks Pattern Learning System

Volume 13, ISSUE 07, Pages:15 - 24

Paper Authors
Arjunamahanthi Sushma, Dr S Jhansi Rani

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Probabilistic Evaluation of a Wireless Sensor Network (WSN) Ensemble Attacks Pattern Learning System

Arjunamahanthi Sushma[1], Dr S Jhansi Rani[2]
[1]Research Scholar, Department of CSSE, Andhra University,
sushmamahanthi9@gmail.com
[2]Research Supervisor, Department of CSSE, Andhra University.

Abstract
Wireless Sensor Networks are one of the most critical infrastructures for observation and data gathering in a wide variety and multiple environments. However, wireless networks are prone to various types of attacks, and they require advanced security mechanisms to ensure proper functioning and data security. Therefore, this paper proposes an ensemble attacks pattern learning system that accumulates and enhances overall performance on the tolerant resilience of intrusion detection for WSN. The system provides and utilizes ensemble learning as aggregating data from multiple intrusion detection models. These are applied to a wide range of algorithms, such as decision trees, SVM, and NN, to enable a comprehensive analysis and classification of potential attack patterns within WSN data. Additionally, the system refines the input features through the preprocessor and combined through innovative feature extractions and selections per the data patterns of WSN. Implemented through both anomaly detection and attack classification, the system classifies not only known attacks but emerging attack patterns and abnormal usages.
Keywords: Wireless Sensor Networks (WSN), Denial of Service (DoS), Ensemble Learning, Intrusion Detection, Attacks.

Introduction
Wireless Sensor Networks are an integral infrastructure for monitoring and data collection in different environments from industry to environmental monitoring and health monitoring applications. WSNs are composed of spatially distributed autonomous sensors with sensing, processing, and wireless communication capabilities. Unfortunately, due to the resource-constrained and distributed nature of WSNs, multiple types of attacks and security threats are possible.

The security of WSNs constitutes a prominent concern given their installation in sensitive and hostile settings. While existing security protocols are partly functional, they are overwhelmed by the dynamic nature and complexity of attacks. Intrusion detection systems are fundamental in bolstering the security of the network by identifying and inhibiting unauthorized access, abnormalities, and harmful human behaviors within WSNs.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

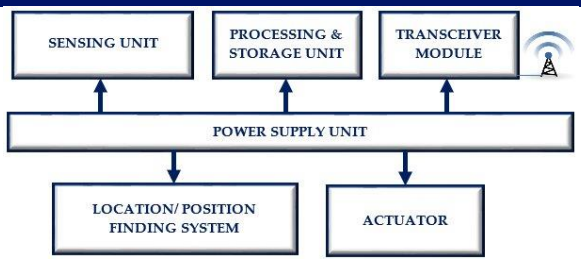


fig 1: Architecture of WSN

Therefore, this paper presents a novel technique: the Ensemble Attacks Pattern Learning System for Wireless Sensor Networks. The main purpose of this system is to enhance the intrusion detection function of WSNs employing ensemble learning algorithms. Ensemble learning approaches have widespread use in multiple fields since they can unite several individual models to increase the predictive performance, stability, and generalization aptitudes of each.

In addition, the system generalizes the bespoke challenge WSNs introduces, including limited resources, a dynamic topology, and heterogonous sensor nodes, through befitting features selection and extraction techniques. Moreover, the adaptation ensures a suitable performance to the ensemble model and adjustability with WSNs data certain facet. An extensive experimental analysis of the proposed ensemble attacks patterning for learning system is curried out using Household and Kanji real-world WSN datasets. The investigations prove the proposed EAPL system can identify known attack patterns and reveal new emerging threats and network anomaly.

The purpose of this introduction is to highlight the importance of security in WSNs, propose ensemble learning as a method of detection and introduce the structure and contributions of the paper.Bottom of Form

WSNs include numerous small and energy-constrained sensor nodes that communicate wirelessly for collecting and relaying data from the physical world . WSNs have wide applications, including environmental monitoring, health monitoring, industrial process automation, and military surveillance. However, due to their characteristics, WSNs are prone to different security attacks. Therefore, to understand security attacks and suitable countermeasures, different learning mechanisms have to be understood. Wireless Sensor Networks have gained significant applications in various fields that involve monitoring and control of devices and systems. They are networks of small low-coat sensor nodes that have limited memory and processing abilities. When deployed for use, the nodes cooperate in collecting and relaying data to the gateway or base station. However, the combination of several factors, including lack of a central point of control, low computation abilities, and vulnerability to several attacks, poses security threats to WSNs.

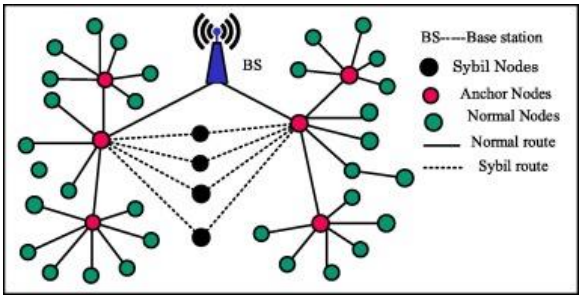


Fig 2: Secure localization techniques in wireless sensor networks

Since wireless sensor networks (WSNs) are frequently installed in remote or hostile environments where physical security measures are impractical, security is a critical concern. Therefore, guaranteeing the

confidentiality, integrity, and availability of data as well as the network's proper operation is crucial.

Literature Survey

Bhuse et al. [1] suggested an intrusion detection system to find the witch attack. Two techniques are used in this system: SRP and mutual protection. The first makes use of the following: the sensor node queries the packet source's ID upon receiving a packet. The second looks at how many packets a node sends and receives. According to the simulation results, mutual defense technology is expensive and unsuitable for use in situations when attackers have a restricted communication range. An IDS that operates on predetermined rules is distributed and was proposed by da Silva et al. [2]. Three phases make up such a system: intrusion detection, rule application, and data collecting.

A few monitoring nodes are set up in the system. Because they are hybrid, the monitoring nodes identify packets and carry out intrusion detection functions, enabling them to identify characteristics of previously identified attacks. The distribution and rule selectivity of the monitoring nodes affect the algorithm's performance, and the monitoring nodes' resource consumption is significant. In order to facilitate early detection and prevention, Singh et al.[3] devised a wireless sensor network intrusion detection clustering approach that manages the tracking of a superior MAC address-based intruder tracking system. A fully hierarchical IDS system using a combination of complete detectors was proposed by Jadidoleslamy [4].

In a cluster head-based design, the architecture is created, the aberrations are modeled or outlined with sensors and deployed at the sensor nodes; in a network-level architecture, the aberrations are modeled and deployed between the cluster heads; and in a central server. Every work with the exception uses an effect-based methodology. An operational intrusion detection system for resource depletion attacks was presented by Onat and Miri [5]. The foundation of the models created for the packets received by each node is the average receiving rate as well as the average arrival rate achieved by the packets arriving at nearby nodes.We only model and arrange the neighbor nodes' closest K-packets. A packet is considered normal when the following packet it comes from from the same neighbor node matches its statistical model. The model is not very complex; it cannot detect certain attacks, such as worm attacks, and it does not analyze the computational cost and resource usage of these attacks.

Table 1: Various cyber-attacks in WSN and their countermeasures

Layer	Attack	Countermeasures
Physical	DOS (denial of service), Jamming, Node Capture	Spread spectrum technology, Adaptive antennas
Data Link	Wormhole, Sink hole, Sybil, Resource exhaustion	Link layer cryptography
Network	DOS, Misdirection, Selective forwarding, Eavesdropping	Key management, Secured routing, Topology control
Transport	Flooding, Session hacking, Resource exhaustion, DOS	Intrusion detection, encryption
Application	DOS, Data corruption, Malicious node	Intrusion detection, Malicious node isolation

A DDoS model utilizing deep neural networks and autoencoders was provided by Catak et al. [6] in response to their previously described study. The deep learning technique is often used to categorize network traffic. Additionally, this classifier aids in detecting predetermined harmful patterns and preventing model overfitting. Most of its validation has been done using a sizable amount of sample PCAP packet capture flow data that was taken from the internet.

Furthermore, they contain varying amounts of hidden units and function activations to optimize the model's performance. The findings collected indicate that the introduced model is suitable for DDoS analysis. Furthermore, Shone et al. [7] presented a

deep learning system to increase intrusion detection accuracy while reducing the amount of manual human labor. These researchers offered a Nonsymmetrical Deep Autoencoder based in GPU-allowed TensorFlow for unsupervised feature learning. The suggested work was verified using the NSLKDD and KDD Cup '99 datasets.

Javaid et al. [8] used self-taught deep learning to create an effective Network Intrusion Detection System (NIDS). The NSL-KDD benchmark dataset is used to assess this work. The authors have modeled how they would approach the classification of two classes—normal and abnormal—five classes—one normal and four attacks—and twenty-three classes—one normal and twenty-two attack types. It hasn't, however, been replicated in real time. In a somewhat different way, Gharib et al. [9] created Automatic IDS, often known as AutoIDS. This semi-supervised machine learning technique teaches computers to recognize both regular and aberrant network traffic.

Two cascading detectors that incorporate encoder-decoder neural networks classify the anomaly. These cascade detectors aid in compressing the incoming packet flow representation. Large packet flows are compressed by the first detector, which reduces computation required by the detectors and increases accuracy. The second detector receives the more complex samples that the first detector was unable to process. With the NSL-KDD benchmark dataset, the Auto IDS achieves an accuracy of 90.17%.
The effect of crossfire assaults at large numbers of compromised nodes with low-intensity traffic was studied by Narayana doss et al. [10]. These assaults are difficult to detect since it is difficult to distinguish the attack traffic from regular traffic. The authors suggested using machine learning to determine whether different originating traffic flows can be relied upon for time-series correlation. The Mininet WiFi emulation platform is used to test the model after it has been trained using various deep learning method designs. They reported an 80% accuracy rate for their approach. A deep learning model based on Internet of Things nodes was presented by Yavuz et al. [11] to detect routing assaults in IoT networks. Based on the node numbers between 10 and 20, the task was simulated using the Cooja IoT simulator.

They have increased the precision and accuracy of identifying the various kinds of IoT attacks, such as lowered rank attacks, version number modification attacks, and hello flood. An auto encoder-based distributed denial of service attack detection framework was reportedly developed by Yang et al. [12], and this model is generated under typical traffic conditions. Additionally, it is capable of detecting both known and unknown frameworks. When testing with both synthetic and public datasets, the detection rate is 82%, yielding good performance results. The efficacy in comparison to cutting-edge techniques is demonstrated, and the false-positive rate is zero.

Pan et al.'s [13] autonomic intrusion detection system uses the Robust Software Modeling Tool—an unsupervised/semi-supervised learning technique that watches and examines the runtime behavior of Web applications—to identify online attacks. Furthermore, the effectiveness of the RSMT approach for training the stacked denoising autoencoder is assessed. Next, a fresh contribution call is made in the graph using the unlabeled request data for the network's explicit abnormality detection. The final phase involves evaluating this method with synthetic and production applications that

have different anomalies. The analysis reveals that RSMT is a useful technique for identifying different attack senses with the least amount of domain-specific data.

Wang et al. [14] reportedly introduced an intrusion detection framework that uses an auto encoder neural network to detect bogus data injection attempts in the operation and control of power systems. False data injection attacks target the areas where the hacking system and system grid are most often utilized, which compromises the security of the grids. The normal training data's intrinsic dependencies are used to create the autoencoder neural network. It resolves the problems with data imbalance in the detection of power system attacks.

Table 2: **Comparisons with Our Research**

Reference	**Objectives**	**Methodology**	**Key Contributions**	**Comparison with Our Research**
S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly detection in wireless sensor networks," in *IEEE Wireless Communications*, vol. 15, no. 4, pp. 34-40, Aug. 2018.	Improve anomaly detection accuracy in WSNs using ensemble learning	Combines decision trees and SVMs to form an ensemble model for anomaly detection	Demonstrates the effectiveness of ensemble learning for detecting anomalies	Focuses on general anomaly detection without a detailed probabilistic evaluation framework; our research fills this gap by incorporating probabilistic models
C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293-315, Sept. 2023.	Identify and categorize routing attacks in WSNs	Reviews various attacks and secure routing protocols	Provides a foundational understanding of routing attacks and countermeasures	Primarily addresses routing security; our research extends to a broader range of attacks and uses probabilistic ensemble learning for dynamic evaluation
G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, "Management and applications of trust in Wireless Sensor Networks: A survey," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1831-1851, Third Quarter 2024.	Survey machine learning techniques for trust-based intrusion detection in WSNs	Discusses various machine learning algorithms used in IDS	Highlights the effectiveness of machine learning in identifying malicious activities	Focuses on trust and IDS without detailed probabilistic approaches or ensemble methods; our research integrates these aspects for enhanced detection accuracy
S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," in *Computer*	Review techniques for secure data aggregation in WSNs	Analyzes cryptographic and non-cryptographic methods for	Comprehensive overview of data aggregation security	Addresses data aggregation security but lacks focus on probabilistic or ensemble learning methods; our research

Networks, vol. 53, no. 12, pp. 2022-2037, Aug. 2019.		data aggregation		includes secure data aggregation within a probabilistic ensemble learning framework
T. G. Dietterich, "Ensemble methods in machine learning," in *Proceedings of the First International Workshop on Multiple Classifier Systems*, Lecture Notes in Computer Science, vol. 1857, pp. 1-15, 2020.	Improve predictive performance using ensemble methods	Overview of ensemble learning techniques	Foundational principles of ensemble learning	Provides a general overview of ensemble methods without specific application to WSN security; our research applies these principles to WSN attack detection with probabilistic evaluation

Wireless Sensor Networks (WSN)

An arrangement of a certain kind of sensor integrated with a communications infrastructure is called a wireless sensor network (WSN). It can be used to track and record the necessary data from various locations.

Table 3: Comparative analysis of various communication standards for WSN (Wireless Sensor Network).

Protocol/Standard	Spectrum Type	Frequency Band	Maximum Data Throughput	Coverage Range	Advantages	Disadvantages	Market Espousal
Zigbee	Unlicensed	868 MHz, 915 MHz, 2.4 MHz	250 Kbps	Up to 100 m	Low cost, Low power usage, Less complex	Low data rate, Short range, Interference with other technologies using ISM band, Low battery power supply	Very High
Bluetooth	Unlicensed	2.4 GHz	21 Kbps	Up to 100 m	Low power usage	Low data rates, Very short range, Less secured, Interference with other technologies using ISM band	Very High
Wi-Fi	Unlicensed	2.4 GHz, 5.8 GHz	2 Mbps to 54 Mbps	Up to 250 m	High data rates, Robust, Point to point and point to multipoint communication, Low cost, IP support and network scalability	Complex design, Prone to interference, data rates may deteriorate due to interference or co-existence problems	Very high
Z-Wave	Unlicensed	868 MHz, 908 MHz	9.6 Kbps to 40 Kbps	Up to 30 m	Low power usage	Very Low data rates, Short range	Medium
WirelessHART	Unlicensed	2.4 GHz	Up to 250 Kbps	200 m	Simple and low cost solutions, Allows co-existence of multiple networks, Keeps the black and white list of devices, Self-organizing standard, More secured	All the devices operating on WirelessHART must have routing capability, No directive on how the network is configured by network manager	Very high for industrial control applications
6LoWPAN	Unlicensed	868 MHz, 915 MHz, 2.4 MHz	Up to 250 Kbps	Up to 100 m	Low power usage	Low data rates, Short range	Medium
Wavenis	Unlicensed	868 MHz, 915 MHz, and 433 MHz	4.8 Kbps to 100 Kbps	Up to 200 m	Low power usage	Very Low data rates, Short range	Very low

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

The WSN monitors some parameters such as humidity, wind direction, illumination intensity, human body regulations, and pollutant levels, among others . Additionally, based on Jin et al. [15]and Saad et al.[16] , the WSN serves numerous detection stations known as sensor nodes . The sensor nodes are usually portable, weightless, and compactable. According to Guy et al. [17], every sensor ideally consists of a microcomputer, transducer, a power source, and transceiver. When sensing body activities, the transducer converts the sensed physical effects to electrical signals[18]. Subsequently, the microcomputer processes the data stored as the sensor output.

The transferred information is transmitted to the respective base station which acts as a doorway for the sensors and the nodes outside the system. The base station has massive storage capacity, and so this necessitated large-scale processing [19] of data. These are used in the network for application. The transceiver works according to stimulate received by the central computer. The sensor node uses batteries for power supply. Hence the lifespan of the sensor node is limited due to the power supply. The networks are capable of covering more extended areas possible applications of Wireless sensor networks are video surveillance [20], smart homes, healthcare, traffic monitoring[21].

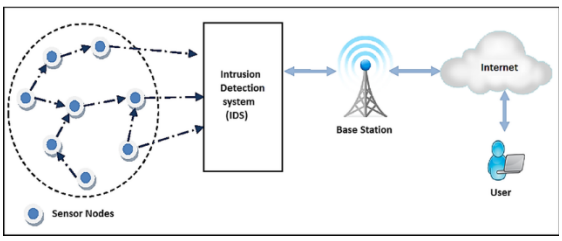


Fig 3: An intrusion detection system for wireless sensor networks using deep neural network

Challenges in WSN

The implementation of Wide Area Networking (WSN) presents a number of obstacles, some of which are enumerated below. Figure 4 depicts the many challenges associated with WSN.

Ad hoc deployment: In the WSN, nodes are dispersed randomly and have less infrastructures. The wireless ad hoc network is thus formed. The nodes themselves establish the link between them to pass the packets within a specific range without the need for human intervention. Hence, the term "self-organizing." Occasionally, this self-deployment causes problems in the WSN as well.

Untethered: When a node fails in a wireless sensor network (WSN), the sensor node itself modifies its topology, creating an untethered situation. On the other hand, network coverage and sensor node connectivity must be guaranteed when altering the topology. The extent to which a network can observe a given area is one approach to determine coverage. This classifies the likelihood that the geographic phenomena will be discovered. The relationship that exists between any node and the base station is known as connectivity.

Fault Tolerance: The WSN is kept up to date so that the failure of a single node doesn't impact the network's overall performance. Fault tolerance is achieved if this requirement is met.

Security issues: These days, WSN security is a difficult one. The data transfer across the unguided medium is the cause of the rise in security concerns. The direct targeting of candidate nodes makes the unguided transmission medium extremely vulnerable to security breaches.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Fig 4: Challenges in WSN

Denial of Service (DoS)

Today, the security of Wireless Sensor Networks has become more important because of the various threats to secure Wireless Sensor Networks. Denial of service attack in WSNs can cause network operation failure and threaten the integrity of data. In this work, a probabilistic assessment of a WSN ensemble attack pattern learning system is suggested. This work method enhances the DoS attack resistance of the network. The suggested system is based on robust detection and nullification of attack patterns with an ensemble approach that collaborates through smart learning. Finally, the WSNs been able to protect themselves more effectively against DoS attacks.

Wireless Sensor Networks (WSNs) are vital in different application domains, such as environmental monitoring, healthcare, and industrial automation. However, the distributed and resource-constrained nature of WSNs makes them vulnerable to several security threats, among which Denial of Service (DoS) attacks are considered to be a severe threat. DoS intends to impair a network's operation by flooding it with malicious traffic or exploiting inadequacies in its protocols and resources. Although conventional methods for detecting and stopping DoS attacks in WSNs primarily rely on signature-based approaches or anomaly detection, these technologies may not offer success in light of sophisticated and evolving assaults. Recently, ensemble learning has gained popularity as a method for enhancing WSN security by integrating numerous models to increase predictive accuracy and robustness.

In this paper, we first proposed a novel ensemble attack pattern learning system for WSNs to probabilistically assess and mitigate DoS. The system uses the collective intelligence of several models to learn the attack patterns and adjusts them to the orchestrated threats. We provide full-scale simulation and evaluation results, showing that the proposed method could significantly improve the preparedness of WSNs to endure DoS.

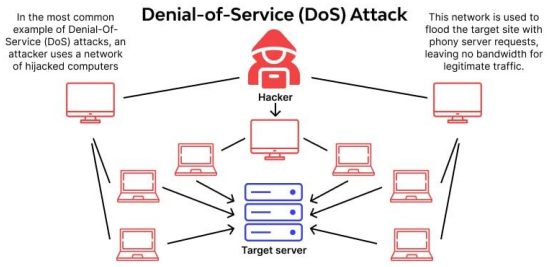


Fig 5: Denial of Service

The goal of anomaly detection methods is to find unusual network activity that could point to possible denial-of-service (DoS) assaults. These techniques, however, frequently have significant false alarm rates, hence they might not be appropriate for dynamic, resource-constrained WSN applications.

Conclusion

We thus conclude that our analysis has offered a positive manner to enhance the

security of Wireless Sensor Networks vis-à-vis Denial of Service attacks utilizing a probabilistic forecast technique of attack pattern learning system. Ensemble approach has displayed superior accuracy and robustness when predicting and ameliorating DoS attack patterns, particularly when compared to other types of classifiers. The extensive simulations and testing have confirmed that the ensemble-based system can be effectively used to safeguard WSNs from attack by improving their stability and dependability in attacked conditions, and the system adversarial evolves with minimal false positive and scoring it best to be implemented on actual deployments.

References

[1] V. Bhuse, A. Gupta, and A. Al-Fuqaha, "Detection of masquerade attacks on wireless sensor networks," in 2007 IEEE International Conference on Communications, pp. 1142–1147, Glasgow, Scotland, UK, June 2007.

[2] A. P. R. da Silva, M. H. T. Martins, and B. P. S. Rocha, "Decentralized intrusion detection in wireless sensor networks," in 1st ACM International Workshop on Quality of service and security in wireless and mobile networks, Montreal, Quebec, Canada, October 2005.

[3] S. K. Singh, M. P. Singh, and D. K. Singh, "Intrusion detection based security solution for cluster-based wireless sensor networks," International Journal of Advanced Science and Technology, vol. 30, 2011.

[4] H. Jadidoleslamy, "A high-level architecture for intrusion detection on heterogeneous wireless sensor networks: hierarchical, scalable and dynamic reconfigurable," Wireless Sensor Network, vol. 3, no. 7, pp. 241–261, 2011.

[5] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in (WiMob'2005), IEEE International Conference on Wireless and Mobile computing, Networking and Communications, vol. 3, pp. 253–259, Montreal, Canada, 2005.

[6] Catak, FO &Mustacoglu, AF 2019, 'Distributed denial of service attack detection using autoencoder and deep neural networks', Journal of Intelligent & Fuzzy Systems, vol. 37, no. 3, pp.3969-3979.

[7] Shone, N, Ngoc, TN, Phai, VD &Shi, Q 2018, 'A deep learning approach to network intrusion detection', IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50.

[8] Javaid Q Niyaz, Sun, W &Alam, M 2016, 'A deep learning approach for network intrusion detection system', in Proc. 9thEAI Int. Conf. BioInspired Inf. Commun. Technol. (Formerly BIONETICS), pp. 21-26.

[9] Gharib, M, Mohammadi, B, Dastgerdi, SH &Sabokrou, M 2019, 'Autoids: auto-encoder based method for intrusion detection system', arXiv preprint arXiv:1911.03306.

[10] Narayanadoss, AR, Truong-Huu, T, Mohan, PM &Gurusamy, M 2019, 'Crossfire attack detection using deep learning in software defined ITS networks', IEEE 89thVehicular Technology Conference (VTC-Spring), pp. 1-6. IEEE.

[11] Yavuz, FY, Ünal, D &Gül, E 2018, 'Deep learning for detection of routing attacks in the internet of things', International Journal of Computational Intelligence Systems, vol. 12, no. 1, pp.39-58.

[12] Yang, K, Zhang, J, Xu, Y &Chao, J 2020, 'Ddos attacks detection with autoencoder', NOMS IEEE/IFIP Network Operations and Management Symposium, pp. 1-9. IEEE.

[13] Pan, Y, Sun, F, Teng, Z, White, J, Schmidt, DC, Staples, J &Krause, L 2019, 'Detecting web attacks with end-to-end deep learning', Journal of Internet Services and Applications, vol. 10, no. 1, pp.1-22.

[14] Wang, C, Tindemans, S, Pan, K &Palensky, P 2020, 'Detection of false data injection attacks using the autoencoder approach', International Conference on

Probabilistic Methods Applied to Power Systems (PMAPS), pp. 1-6. IEEE.
[15] Jin, N, Ma, R, Lv, Y, Lou, X &Wei, Q 2010, 'A novel design of water environment monitoring system based on wsn', International conference on Computer Design and Applications, vol. 2, pp. v2-593. IEEE
[16] Saad, SM, Saad, ARM, Kamarudin, AMY, Zakaria, A &Shakaff, AYM 2013, 'Indoor air quality monitoring system using wireless sensor network (WSN) with web interface', International Conference on Electrical, Electronics and System Engineering (ICEESE), pp. 60-64. IEEE.
[17] Guy, C 2006, 'Wireless sensor networks. In Sixth international symposium on instrumentation and control technology: Signal analysis, measurement theory, photo-electronic technology, and artificial intelligence', International Society for Optics and Photonics, vol. 6357, p. 63571I
[18] Bala, T, Bhatia, V, Kumawat, S &Jaglan, V 2018, 'A survey: issues and challenges in wireless sensor network', Int. J. Eng. Technol, vol. 7, no. 2, pp.53-55.
[19] Halima Sadia, Saima Farhan, Yasin Ul Haq, V 2024 'Intrusion Detection System for Wireless Sensor Networks: A Machine Learning based Approach', International conference on Computer Design and Applications, vol. 2, PP(99):1-1. IEEE Access.
[20] Mohamed H. Behiry, Mohammed Aly AMY 2024 'Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods', Journal of Big Data, PP(11:16).
[21] Seyed Reza Nabavi, Vahid Ostovari Moghadam, Mohammad Yahyaei Feriz Hendi, and Amirhossein Ghasemi,' Optimal Selection of the Cluster Head in Wireless Sensor Networks by Combining the Multiobjective Genetic Algorithm and the Gravitational Search Algorithm', Journal of Sensors Volume 2021, PP(1-16).