

















ORIGINAL

Abnormality detection in wireless medical sensor networks using machine learning model

Detección de anomalías en redes inalámbricas de sensores médicos mediante aprendizaje automático

Bekhruzbek Kadirov¹  , Janna Nazarova²  , Nigora Alikulova³  , Rasuljon Shermatov⁴  , Sokhiba Narkulova⁵  , Utkir Farmonov⁶  , Nodira Alimukhamedova⁷  

¹Bukhara State Medical Institute named after Abu Ali ibn Sino. Bukhara, Uzbekistan.

²Center for the Development of Professional Qualifications of Medical Workers of the Ministry of Health of the Republic of Uzbekistan. Uzbekistan.

³Center for the development of professional qualification of medical workers. Tashkent Uzbekistan.

⁴Fergana Medical Institute of Public Health, Republic of Uzbekistan. Ferghana.

⁵Samarkand State Medical University. Samarkand, Uzbekistan.

⁶Jizzakh State Pedagogical University. Uzbekistan.

⁷Tashkent Institute of Irrigation and Agricultural Mechanization Engineers National Research University. Tashkent, Uzbekistan.


Cite as: Kadirov B, Nazarova J, Alikulova N, Shermatov R, Narkulova S, Farmonov U, et al. Abnormality detection in wireless medical sensor networks using machine learning model. Health Leadership and Quality of Life. 2024; 3:180. <https://doi.org/10.56294/hl2024.180>


Submitted: 27-02-2024

Revised: 17-06-2024

Accepted: 13-10-2024

Published: 14-10-2024

Editor: PhD. Prof. Neela Satheesh 

Corresponding Author: Bekhruzbek Kadirov 

ABSTRACT

The monitoring of long-term physiological parameters in hospital settings is costly and requires the presence of important healthcare personnel. Wireless medical sensor networks (WMSNs) can be used to monitor patients' physiological data, making healthcare applications one of the most promising areas for wireless sensor networks. The remote management of patient healthcare may change with the introduction of wireless sensor devices as a part of a Wireless Body Area Network (WBAN) integrated within an overall e-Health system. A crucial component of a comprehensive health monitoring network can include tiny sensor devices that are positioned within or on top of the human body. Although it should be efficient in its process, an energy-efficiently built WBAN and WMSN should have no effect on the patient's mobility or way of life. WBAN technology can be used in a patient's residence, a hospital, or a health care facility. Patients' privacy is jeopardised when new technologies are implemented in healthcare applications without proper security considerations. Security is an essential prerequisite for healthcare apps since physiological data about an individual is extremely sensitive, particularly when it comes to patient privacy.

Keywords: Wireless Medical Sensor Networks; Wireless Body Area Network; Patient Healthcare; Attack.

RESUMEN

La monitorización de parámetros fisiológicos a largo plazo en entornos hospitalarios es costosa y requiere la presencia de personal sanitario importante. Las redes inalámbricas de sensores médicos (WMSN) pueden utilizarse para monitorizar los datos fisiológicos de los pacientes, lo que convierte a las aplicaciones sanitarias en una de las áreas más prometedoras para las redes inalámbricas de sensores. La gestión a distancia de la atención sanitaria a los pacientes puede cambiar con la introducción de dispositivos sensores inalámbricos como parte de una red inalámbrica de área corporal (WBAN) integrada en un sistema global de sanidad electrónica. Un componente crucial de una red global de vigilancia sanitaria puede incluir diminutos

dispositivos sensores colocados dentro o encima del cuerpo humano. Aunque debe ser eficiente en su proceso, una WBAN y una WMSN construidas con eficiencia energética no deben afectar a la movilidad ni al modo de vida del paciente. La tecnología WBAN puede utilizarse en la residencia de un paciente, en un hospital o en un centro sanitario. La privacidad de los pacientes se pone en peligro cuando las nuevas tecnologías se implantan en aplicaciones sanitarias sin las debidas consideraciones de seguridad. La seguridad es un prerequisite esencial para las aplicaciones sanitarias, ya que los datos fisiológicos de una persona son extremadamente sensibles, sobre todo cuando se trata de la privacidad del paciente.

Palabras clave: Redes Inalámbricas de Sensores Médicos; Redes Inalámbricas de Área Corporal; Atención Sanitaria a Pacientes; Ataque.

INTRODUCTION

The development of computing and communication technologies has accelerated. In many facets of daily life, the capacity to coordinate and communicate between various devices through wireless communication has had a profound effect.⁽¹⁾ One field that has evolved slowly is medicine. Regarding the security and integrity of the data generated and kept up to date in the systems being built to assist physicians and patients in meeting their needs, there are several worries.⁽²⁾ Applying many of the most modern wireless communication innovations to issues in the medical field requires careful consideration of patient safety and privacy.⁽³⁾ The general public is concerned about the processing, transmission, and storage of personal medical information in below figure 1. The veracity and correctness of the medical data that they receive worry clinicians. It is beneficial to look into the security vulnerabilities that are now present in wireless networks and the ways in which they have been fixed in order to allay worries about the use of this technology for patient monitoring.⁽⁴⁾ Applying the knowledge gathered from wireless deployments will allow clinical systems' needs and concerns to be met, ensuring staff and patient safety. The security concerns must be resolved before wireless technology, which will greatly improve clinical care, is implemented in the clinical setting.⁽⁵⁾ The capacity to remotely follow patient information will allow clinicians to see a fuller picture of their patients' health. The longer period of time that patient data can be collected will improve knowledge of the effects of medical interventions and enable more thorough improvement of those interventions to produce better overall outcomes or customized interventions for every patient.⁽⁶⁾ Thanks to technology, doctors will be able to determine if a patient's health is steady or decreasing over an extended period of time.

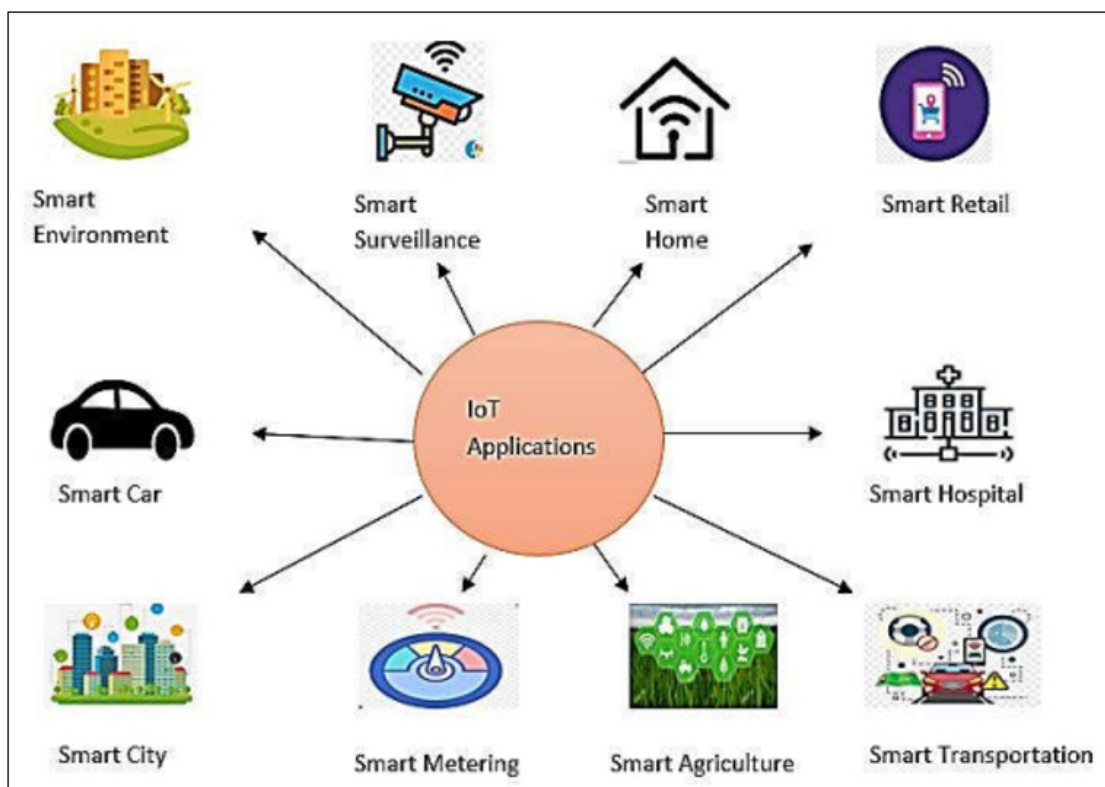


Figure 1. Applications of IoT

Research Background

Wireless Medical Sensor Networks (WMSN) are networks of medical sensors that are positioned within or outside of the body to monitor a patient's vital signs and send the information they detect in a timely manner, all without the need for human involvement, to a distant site.⁽⁷⁾ The patient's movements within their home, their body temperature, and other biomedical data like oxygen saturation can all be monitored by a MWSN.⁽⁸⁾ Following discharge from the hospital, a patient's vital signs, including heart rate, temperature, blood pressure, motion or acceleration, pulse oximetry, etc., can be continually monitored. Patients may very well receive very little medication in addition to sensor data, according to data from medical sensor networks.⁽⁹⁾ The drug's delivery would be managed through wireless transmission. Since the patient's medical care and the data collected by a MWSN are so closely linked, all communication needs to be very secure, highly reliable, and simple to access in order to prevent mistakes and guarantee that the patient gets the medication they require when they need it.⁽¹⁰⁾ WMSN can be used to improve the quality of care in a wide range of healthcare applications, including ambulatory monitoring, clinical monitoring, monitoring of vital physiological signals in hospitals, elderly individuals receiving at-home care, monitoring during mass casualty disasters, and more.

⁽¹¹⁾ Wireless Body Area Networks (WBANs) are also useful for other applications, such as patient self-care and sports-person health status monitoring.⁽¹²⁾

The paper's next section is structured as follows: Section 2 provides the main goal and target of the wireless Body Area Networks. Section 3 proposed a novel methodology. Section 4 describes the experiment that was conducted utilizing a novel technique. Section 5 presents the work's conclusion.

Proposed Framework

The field of Artificial Intelligence (AI) is Machine Learning that allows the device or system to enhance the learning capability naturally or without any interaction of an individual.^(13,14) The system can improve its performance through training even in the absence of any programming. Despite being a branch of computer science, machine learning is not like other approaches.⁽¹⁵⁾ Conventional algorithms follow a predetermined series of steps to address an issue. The machine learning algorithms are trained earlier with a massive amount of data in order to create a better diagnosis and decision for the fresh data. The learning algorithm improves significantly if it is frequently taught with a large volume of data. It creates the prediction model using historical data as a result of this training.^(16,17) It is discovered that such a trained algorithm produces accurate predictions and conclusions. Modern technologies take use of machine learning's advantages. Figure 2 shows how BLID is designed. It is composed of three levels, which are explained as follows:

- Unsupervised Layer: the fuzzy membership values are used in the unsupervised layer by the Fuzzy C Means clustering technique to generate the number of clusters.
- Supervised Layer: using fuzzy clusters, the Random Forest and Naïve Bayes classifiers are trained and evaluated in the supervised layer.
- Decision Layer: to help us decide more wisely about the intrusions, we use the Randomised Weighted Majority Algorithm in the decision layer.

Unsupervised Layer

Based on the fuzzy membership function, the fuzzy c-means clustering separates the dataset into a massive number of groups.⁽¹⁸⁾ Within the cluster, the data points are homogeneous, while outside of certain clusters, they are heterogeneous. The data is clustered once the pertinent features have been extracted.^(19,20) Fuzzy C-Means clustering is a text and soft clustering approach that creates various clusters. The fuzzy membership value is used to define the cluster group. The fuzzy membership value is updated recursively in this repetitious approach.

Algorithm: Fuzzy C-Means Clustering

1. Initially, set the closure criteria as 0,001.
2. Select the cluster number (c) haphazardly.
3. Reckon the cluster membership function is calculated.
4. Reckon the Center value is measured.
5. The objective function is estimated.
6. Reiterate steps 3, 4 and 5 until the closure criteria satisfy.

Every piece of data in the dataset is assigned to the proper clusters once this algorithm has been processed. The FCM is used to reduce the bulk of the dataset and its ramifications.^(21,22) It improves the performance of Random Forest and Naïve Bayes classifiers.

Supervised Layer

The simple supervised classification method known as Naïve Bayes employs the fundamentals of the Bayes

theorem.^(23,24) The NB approach assumes the naïve among the examples for every data point in the dataset. The categorisation method that operates under supervision is called Random Forest. Several decision trees are required for the development of Random Forest, as opposed to just one. As implied by the name “forest,” a vast number of trees are needed to create a forest. If the random forest is constructed from more decision trees, its accuracy will increase.⁽²⁵⁾ The quantity of trees determines how resilient the forest is. It uses the output from each decision tree in the random forest to determine the ultimate conclusion. When compared to the outcomes of the random forest, the decision tree’s accuracy is low.

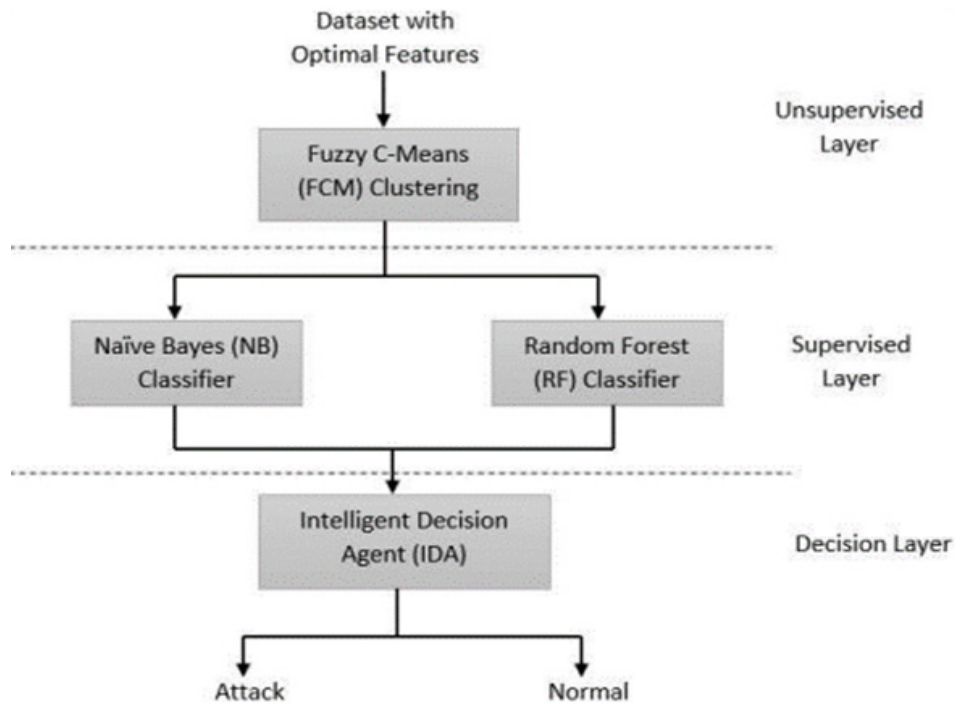


Figure 2. Proposed Framework

Decision Layer

In our suggested approach, we employ the Gushing Randomised Weighted Majority Algorithm (GRWMA) as an Intelligent Decision Agent (IDA) to help choose between Random Forest and Naïve Bayes, the two fundamental classifiers.⁽²⁶⁾ According to the Randomised Weighted Majority Algorithm solves the expert advice dilemma. Two base classifiers are employed in our approach, and each has its own weight. Each classifier makes the prediction for new instances, and it also assigns the label for the predictions and weights for the two classifiers. Every time the classifier correctly predicts a label, it modifies its weight;^(27,28,29) if it predicts a wrong label, the constant factor is penalised. It forecasts which of the two classifiers is the better one.

RESULTS AND DISCUSSION

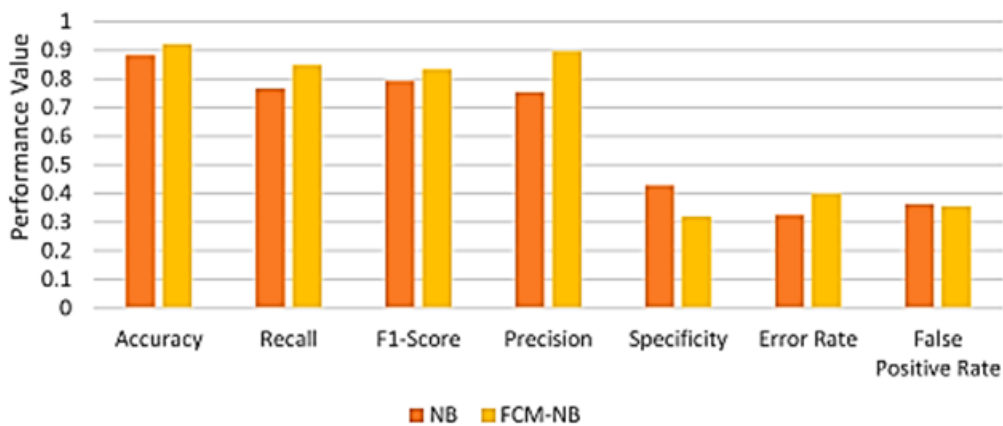


Figure 3. Predictor variables

The evaluation of the performance of the Sinkhole detecting algorithm is done by NS2-simulations. A 600 by 600 metre field is used to simulate a wireless sensor network, with 50 and 400 nodes distributed uniformly at random. The sensors use the IEEE 802.11 MAC protocol and have a 10-meter radio range.

In order to compare the outcomes of different anomaly detection algorithms, we employ four intrusion detection datasets: the IoT Network Intrusion Dataset 2019 and the KDD CUP 99, NSL-KDD, and CICIDS 2017 by Ring et al. The KDD CUP 99 and NSL-KDD datasets contain 23 different attacks across the four categories (DoS, U2R, R2L, and Probe). The six categories of the 15 sub-attacks in the CICIDS 2017 dataset include distributed denial of service, online assault, infiltration, botnet ARES, and brute force. Two devices are used to record the IoT network intrusion dataset: the SKT NUGU (NU 100) and the EZVIZ Wi-Fi camera (C2C Mini O Plus 1080P).

Figure 3 illustrates that FCM-NB achieves 0,92 accuracy, 0,84 recall, 0,83 F1 score, 0,89 precision, 0,31 specificity, 0,39 error rate, and 0,35 false positive rate, while NB achieves 0,88 accuracy, 0,76 recall, 0,79 F1 score, 0,75 precision, 0,48 specificity, 0,32 error rate, and 0,36 false positive rate. Figure 4 illustrates how well the FCM-NB classifier detects the probing and R2L assaults compared to the other two attacks.

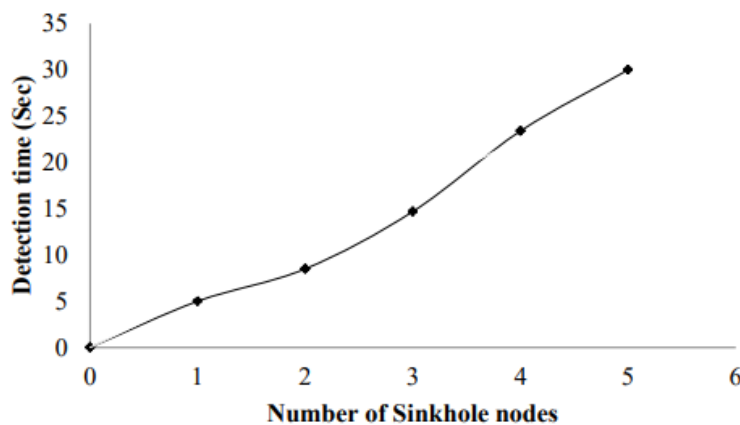


Figure 4. Time taken to identify the intruder sink node

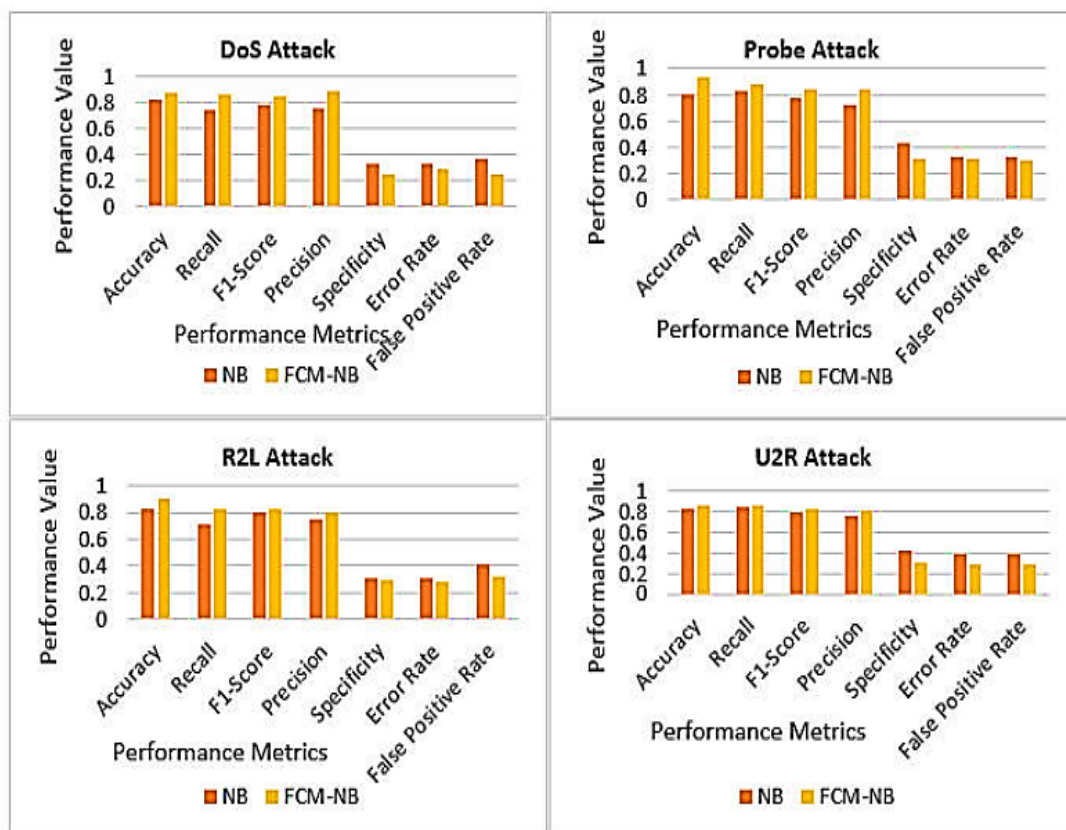


Figure 5. Performance comparison of Distinct Attacks in NB and FCM-NB for KDD CUP 99

The suggested protocol's time taken to identify the invader sink node is depicted in figure 4 graph. Sinkhole attacks, both single and multiple, are used to repeat the protocol. A single sinkhole attack is detected by the protocol in 5 seconds, whereas 5 sinkhole attacks are detected in 30 seconds.

In terms of round count and sinkhole node detection, the suggested algorithm's and CSW's performances are compared. After around six cycles, the suggested method finds every Sinkhole node, as shown in figure 5. One of the key elements of sensor networks is network dependability. The network's ability to detect events during the course of the network's lifetime can be used to establish these QoS parameters. A network's reliability increases with the number of events it is able to report. It is clear from figure 5 that the suggested approach outperforms the current technique in terms of reliability.

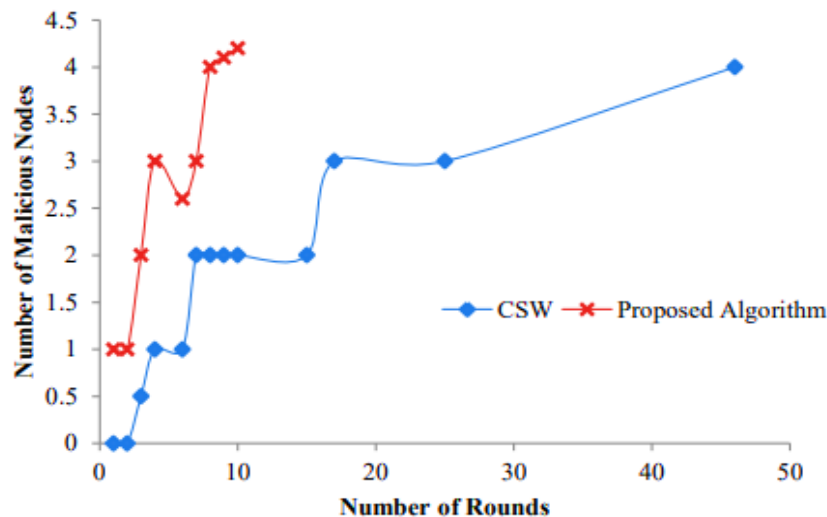


Figure 6. Reliability of the proposed algorithm with CSW

With 400 nodes instead of just 9, the algorithm's detection accuracy remains constant. It reaches its peak when there are a maximum number of nodes because the algorithm is very scalable and performs well even with a wide range of network sizes. Performance is virtually completely unaffected by the size of the network. The variance in detection accuracy as a function of network node count is depicted in figure 6.

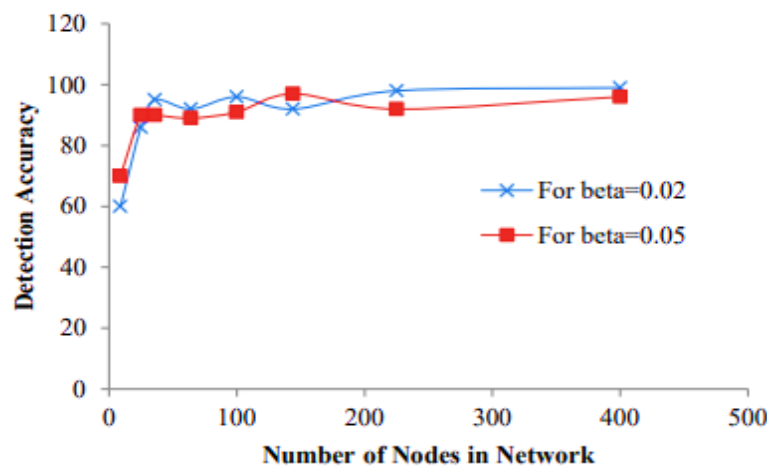


Figure 7. Detection accuracy variation with respect to Number of Nodes

The only factor influencing the sinkhole attack's detection accuracy is the variance in compromised nodes. This occurs as a result of the monitoring time interval influencing the detection accuracy since the attack is evaluated over a period of time. The window of time that a base station needs to gather packets and examine them for indications of intrusion is known as the monitoring interval. Due to the shorter time interval, fewer packets are being gathered, and since packets are discarded at random, it is possible that fewer packets will be dropped during a brief monitoring interval. As a result, no alarm will sound, leading to false negatives.

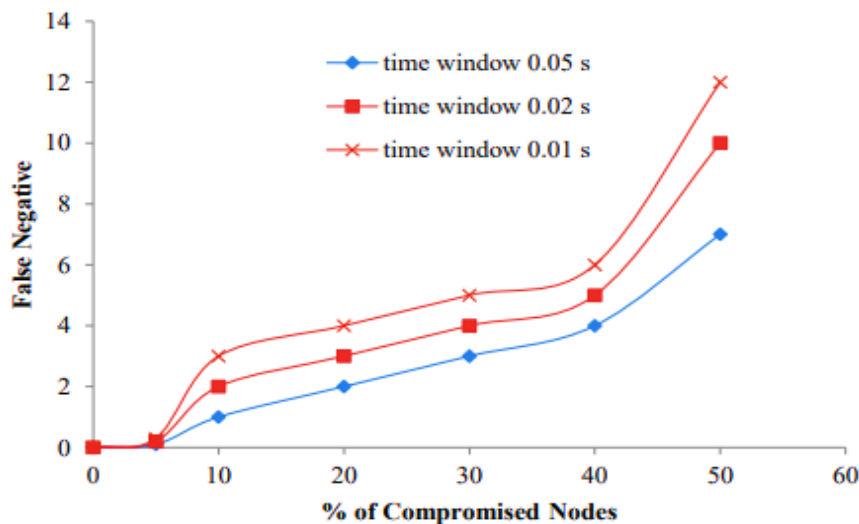


Figure 8. Probability of false negative with Percentage of compromised nodes in various time windows

This condition is less likely to occur when the interval value increases or when nodes initiate a sinkhole attack, i.e., packet drop = 100 %. In the latter situation shown in figure 7, the dropped packets likelihood throughout an interval are fewer, results in a false negative being near to zero and hence, the accuracy of detecting this assault is close to 100 %.

CONCLUSIONS

Security is a major concern in the context of pervasive connection and the Internet of Things. IoT-enabled industries and organizations are increasingly open to assaults. It is difficult for traditional cybersecurity systems to detect zero-day threats. The intruder takes use of the IoT infrastructure's access privileges to obtain useful data. Few security dangers are well-known threats, and few occur over time which is unknown attacks. Using machine learning techniques to provide intrusion detection is an effective strategy to deal with these unmatched problems. In order to lessen the abnormalities in the Internet of Things environment, we created a robust machine learning framework. This is the framework that Bi-Layer Intrusion Detection uses to follow. In the fog node, distributed training is the framework's last achievement.

BIBLIOGRAPHIC REFERENCES

1. Bagwari, Ashish, Jaganathan Logeshwaran, K. Usha, R. Kannadasan, Mohammed H. Alsharif, Peerapong Uthansakul, and Monthippa Uthansakul. "An Enhanced Energy Optimization Model for Industrial Wireless Sensor Networks Using Machine Learning." *IEEE Access* (2023).
2. Ahmad, Rami, Raniyah Wazirali, and Tarik Abu-Ain. "Machine learning for wireless sensor networks security: An overview of challenges and issues." *Sensors* 22, no. 13 (2022): 4730.
3. Feng, Zhen, Jingqi Fu, Dajun Du, Fuqiang Li, and Sizhou Sun. "A new approach of anomaly detection in wireless sensor networks using support vector data description." *International Journal of Distributed Sensor Networks* 13, no. 1 (2017): 1550147716686161.
4. Arfaoui, Amel, Ali Kribeche, Sidi Mohammed Senouci, and Mohamed Hamdi. "Game-based adaptive anomaly detection in wireless body area networks." *Computer Networks* 163 (2019): 106870.
5. Gao, Honghao, Lin Zhou, Jung Yoon Kim, Ying Li, and Wanqiu Huang. "Applying probabilistic model checking to the behavior guidance and abnormality detection for A-MCI patients under wireless sensor network." *ACM Transactions on Sensor Networks* 19, no. 3 (2023): 1-24.
6. Albattah, Albatul, and Murad A. Rassam. "A correlation-based anomaly detection model for wireless body area networks using convolutional long short-term memory neural network." *Sensors* 22, no. 5 (2022): 1951.
7. Kavitha, M., P. V. V. S. Srinivas, PS Latha Kalyampudi, and Singaraju Srinivasulu. "Machine learning techniques for anomaly detection in smart healthcare." In *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 1350-1356. IEEE, 2021.

8. Salem, Osman, Khalid Alsubhi, Ahmed Mehaoua, and Raouf Boutaba. "Markov models for anomaly detection in wireless body area networks for secure health monitoring." *IEEE Journal on Selected Areas in Communications* 39, no. 2 (2020): 526-540.
9. Dwivedi, Rajendra Kumar, Sonali Pandey, and Rakesh Kumar. "A study on machine learning approaches for outlier detection in wireless sensor network." In *2018 8th international conference on cloud computing, data science & engineering (confluence)*, pp. 189-192. IEEE, 2018.
10. Kanev, Anton, Aleksandr Nasteka, Catherine Bessonova, Denis Nevmerzhitsky, Aleksei Silaev, Aleksandr Efremov, and Kseniia Nikiforova. "Anomaly detection in wireless sensor network of the "smart home" system." In *2017 20th Conference of open innovations association (FRUCT)*, pp. 118-124. IEEE, 2017.
11. Mittal, Mohit, Rocío Pérez De Prado, Yukiko Kawai, Shinsuke Nakajima, and José E. Muñoz-Expósito. "Machine learning techniques for energy efficiency and anomaly detection in hybrid wireless sensor networks." *Energies* 14, no. 11 (2021): 3125.
12. Ifzarne, Samir, Hiba Tabbaa, Imad Hafidi, and Nidal Lamghari. "Anomaly detection using machine learning techniques in wireless sensor networks." In *Journal of Physics: Conference Series*, vol. 1743, no. 1, p. 012021. IOP Publishing, 2021.
13. Salem, Osman, Alexey Guerassimov, Ahmed Mehaoua, Anthony Marcus, and Borko Furht. "Sensor fault and patient anomaly detection and classification in medical wireless sensor networks." In *2013 IEEE international conference on communications (ICC)*, pp. 4373-4378. IEEE, 2013.
14. Salem, Osman, Alexey Guerassimov, Ahmed Mehaoua, Anthony Marcus, and Borko Furht. "Anomaly detection in medical wireless sensor networks using SVM and linear regression models." *International Journal of E-Health and Medical Communications (IJEHMC)* 5, no. 1 (2014): 20-45.
15. Pachauri, Girik, and Sandeep Sharma. "Anomaly detection in medical wireless sensor networks using machine learning algorithms." *Procedia Computer Science* 70 (2015): 325-333.
16. Soyipov, S., Khaitov, F., Shukurova, F., Rashidova, K., Aliyeva, M., Yuldasheva, G., Berdiyeva, N., & Jumanov, A. (2024). Digital Democracy: How Technology Can Drive Higher Voter Turnout in Elections. *Indian Journal of Information Sources and Services*, 14(4), 22-28. <https://doi.org/10.51983/ijiss-2024.14.4.04>
17. Stamenkovic, Saša, Stevovic, S., & Stamatovic, Milan. (2019). Res Capacity Increase in EU and Wind Project Sustainability with Case Study on Serbia and Montenegro Market. *Archives for Technical Sciences*, 1(20), 1-11.
18. Turan, C., Gürlek, M., Dağhan, H., Demirhan, S. A., & Karan, S. (2020). First clinical case of the venomous Lessepsian migrant fish *Plotosus lineatus* in the Iskenderun Bay, the Northeastern Mediterranean Sea. *Natural and Engineering Sciences*, 5(1), 50-53. <https://doi.org/10.28978/nesciences.691699>
19. Rojas, J. B., Carrasco, D. N. D., Saldaña, C. M. A., Tananta, C. A. F., Vásquez, A. P., & Jimenez, K. M. A. (2024). Scientific Production on Budget Execution in Latin American Organizations. *Indian Journal of Information Sources and Services*, 14(4), 60-65. <https://doi.org/10.51983/ijiss-2024.14.4.10>
20. Ilić, P., Popović, Z., & Gotovac-Atlagić, S. (2019). Effects of Meteorological Variables on Nitrogen Dioxide Variation. *Archives for Technical Sciences*, 1(20), 65-72.
21. Yalman, E., Federer-Kovacs, G., & Depci, T. (2021). Effect of Two Types of Fly Ash on Rheological and Filtration Properties of Water-Based Drilling Mud. *Natural and Engineering Sciences*, 6(3), 223-236. <http://doi.org/10.28978/nesciences.1036853>
22. Khalikova, R., Musaeva, U., Djuraeva, N., Jumanazarov, U., Sadridinova, F., Khujakulov, A., & Sattorova, Z. (2024). Managing Digital Transformation: Analysing Digitalization of How Firms Attract, Retain, and Develop Digital Skills. *Indian Journal of Information Sources and Services*, 14(4), 147-152. <https://doi.org/10.51983/ijiss-2024.14.4.23>

23. Bekényiová, A., Danková, Z., Hegedüs, M., Mitróová, Z., Dolinská, S., & Znamenáčková, I. (2020). Column Sorption of Toxic Ions in Various Quartz Sand - Packed Columns. *Archives for Technical Sciences*, 1(22), 43-50.
24. Doğdu, S. A., Turan, C., & Depci, T. (2021). Extraction and characterization of chitin and Chitosan from invasive alien swimming crab *Charybdis longicollis*. *Natural and Engineering Sciences*, 6(2), 96-101. <http://doi.org/10.28978/nesciences.970546>
25. Lopez, H. P., Lopez, L. R. V., López, R. J. C., Gonzales, T. V. P., Lozano, S. M., & Ramírez, S. V. L. (2024). Study of Scientific Production on Stress at Work in Organizations. *Indian Journal of Information Sources and Services*, 14(4), 136-140. <https://doi.org/10.51983/ijiss-2024.14.4.21>
26. Karimov, A., et al. (2019). Rethinking settlements in arid environments: Case study from Uzbekistan. *E3S Web of Conferences*, 97, 05052. <https://doi.org/10.1051/e3sconf/20199705052>
27. Karimov, N., et al. (2024). Exploring food processing in natural science education: Practical applications and pedagogical techniques. *Natural and Engineering Sciences*, 9(2), 359-375. <https://doi.org/10.28978/nesciences.1574453>
28. Odilov, A., et al. (2024). Utilizing deep learning and the Internet of Things to monitor the health of aquatic ecosystems to conserve biodiversity. *Natural and Engineering Sciences*, 9(1), 72-83. <https://doi.org/10.28978/nesciences.1491795>
29. Sasikala, R., Deepthi, K. J., Balakrishnan, T. S., Krishnan, P., & Ebenezar, U. S. (2024, June). Machine Learning-Enhanced Analysis of Genomic Data for Precision Medicine. In *2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0* (pp. 1-5). IEEE. <https://doi.org/10.1109/OTCON60325.2024.10687539>

FINANCING

No financing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Data curation: Bekhruzбек Kadirov, Janna Nazarova, Nigora Alikulova, Rasuljon Shermatov, Sokhiba Narkulova, Utkir Farmonov, Nodira Alimukhamedova.

Methodology: Bekhruzбек Kadirov, Janna Nazarova, Nigora Alikulova, Rasuljon Shermatov, Sokhiba Narkulova, Utkir Farmonov, Nodira Alimukhamedova.

Software: Bekhruzбек Kadirov, Janna Nazarova, Nigora Alikulova, Rasuljon Shermatov, Sokhiba Narkulova, Utkir Farmonov, Nodira Alimukhamedova.

Drafting - original draft: Bekhruzбек Kadirov, Janna Nazarova, Nigora Alikulova, Rasuljon Shermatov, Sokhiba Narkulova, Utkir Farmonov, Nodira Alimukhamedova.

Writing - proofreading and editing: Bekhruzбек Kadirov, Janna Nazarova, Nigora Alikulova, Rasuljon Shermatov, Sokhiba Narkulova, Utkir Farmonov, Nodira Alimukhamedova.