Anomalous Cluster Heads and Nodes in Wireless Sensor Networks

Sare Gorgbandi*[a], Reza Brangi[b]

Faculty of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran. Miracel@gmail.com*[a], Rbrangi@iust.ac.ir[b]

ABSTRACT

The majority of wireless sensor network (WSN) security protocols state that a direct connection from an attacker can give them total control of a sensor node. A high level of security is necessary for the acceptance and adoption of sensor networks in a variety of applications. In order to clarify this issue, the current study focuses on identifying abnormalities in nodes and cluster heads as well as developing a method to identify new cluster heads and find anomalies in cluster heads and nodes. We simulated our suggested method using MATLAB tools and the Database of the Intel Research Laboratory. The purpose of the performed simulation is to identify the faulty sensor. Using the IBRL database, sensors that fail over time and their failure model is the form that shows the beats in the form of pulses, we find out that the sensor is broken and is of no value. Of course, this does not mean that the sensor is invasive or intrusive. We have tried by clustering through Euclidean distance that identify disturbing sensors. But in this part of the simulation, we didn't have any data that shows disturbing sensors, it only shows broken sensors. We have placed the sensors randomly in a 50 x 50 space and we want to identify the abnormal node.

Keywords: ***Cluster Head, Clustering, Anomaly, Wireless Sensor Network, Security, Node***

1. Introduction

Wireless sensor networks (WSN) are one of the most promising areas of information and communication technology at the moment. This innovative technology offers limitless potential for a variety of uses in several fields such as environmental research, medicinal applications, military, transportation, entertainment, crises management, home security and intelligent spaces. The main limitations of WSNs are their high energy consumption, poor communication, limited computational capacity and scalability [1]. WSNs have been used in numerous practical applications that significantly enhance our quality of life. Security is a major concern because WSNs are so widespread and new technologies have recently been developed [2]. As a possible technology WSNs have attracted a lot of attention. Although various research has focused on WSNs only a few have examined their security vulnerabilities in depth. Systems that don't adhere to security standards may give attackers the opportunity to lower the overall system performance [3]. In hostile environments protecting WSNs against malicious attacks is essential. Due to several resource limits and the unique features of a wireless sensor network the security design for such networks is exceedingly challenging [4]. Due to the open nature of wireless media and the regular interactions between sensor nodes (WSNs) security has been intimately tied to the accuracy of the data and the dependability of the network [5]. Traditional approaches that require significant overhead in processing and communication are not practical in WSNs due to resource limitations in the sensor nodes. Consequently, designing and deploying secured WSNs is a difficult task [6]. Due to their hardware resource limitations, Wireless Sensor Networks (WSNs) continue to face significant issues with regard to energy consumption and security efficiency [7].

The position of each sensor node in Wireless Sensor Networks is one of the most crucial pieces of information. Attackers are especially drawn to this type of information since it exposes the real positions of nodes leaving the entire network open to various types of intrusion [8]. Data in wireless sensor networks can be vulnerable to errors and malicious assaults which makes it unreliable. We must therefore identify abnormal nodes in order to provide a reliable system [9]. Strong spatio-temporal correlations are displayed by many heterogeneous sensors which can be exploited to help with the wireless sensor network's issue with problematic node detection. It has been demonstrated that identifying bogus data injection attacks using corruption in these correlations is successful [10]. In a WSN independent nodes perceive and observe the space around us by observing and feeling things like temperature, sound, vibration, and more. WSN may transport data to base stations (BS) and carry out various sorts of processing including as data gathering, data sensing and data processing. It can also be used to determine the most efficient path for data transmission between nodes and BS [11].

The secret to protecting the energy resources of sensor nodes is effective cluster head (CH) selection in rounds. As a result, ensuring CH selection with the proper security resources without reducing energy efficiency is difficult. The aforementioned trade-off can be resolved by optimizing coverage and energy under the condition that a certain level of security is maintained [12]. The majority of WSNs however are constrained by particular factors such as low processing power and unsupervised environments [13]. Problems with consumption of energy and transmitting patterns that impede efficient data transfer must also be addressed [14]. Data integrity and network node authentication are additional major issues with these

http://dx.doi.org/10.22133/ijwr.2022.343273.1114

Citation. S. Gorgbandi, R. Brangi "Anomalous Cluster Heads and Nodes in Wireless Sensor Networks," *International Journal of Web Research*, vol.5,no.1, pp. 66-73, 2022.

*Coressponding Author

Article History: Received: 20 May 2022 ; Revised: 12 July 2022; Accepted: 3 August 2022

applications. With the exception of military applications, there are some circumstances where data integrity and authentication are more crucial than confidentiality. In many applications, the user wants to be certain that the event they have obtained is accurate before making a crucial decision. As a result, we must build a security protocol that is both efficient and does not require more energy. The difficulty of identifying abnormal occurrences in nodes has long been considered in these networks [15].

The majority of wireless sensor network (WSN) security protocols state that a direct connection from an attacker can give them total control of a sensor node. A high level of security is necessary for the acceptance and adoption of sensor networks in a variety of applications. In order to clarify this issue, the current study focuses on identifying abnormalities in nodes and cluster heads as well as developing a method to identify new cluster heads and find anomalies in cluster heads and nodes. The following are the paper's main contributions: Section 2 evaluated security articles and various techniques for detecting anomalies in sensor nodes. Our proposed method for locating anomalies in sensor and cluster head nodes is presented in Section 3. In Section 4, we use the Intel Research Laboratory Database and MATLAB software to simulate our suggested method. In section 5, 6, 7, we presented the efficiency and accuracy of our proposed method compared to previous methods.

2. Related Work

By expanding a diagrammatic filtering framework, a method for detecting spectral anomalies is proposed. To convey important information about the data measured, this diagram was chosen. A dependency graph-based filtering technique is used to plot diagram signals in sub, normal, and anomalous space while the projected result is used to find anomalies. The distance between the sensors can be used to improve the local performance of anomaly detection in the suggested method, which is applicable to the turbulence of strong parameters and is compatible with a number of scoring criteria. On the other hand, this strategy has a weakness in that the frequency of the near-anomaly may be equal to the desired frequency [16].

For the purpose of identifying sensor node anomalies, techniques based on the generation of predictions for comparison and detection have been presented. This strategy takes into account the temporal and spatial relationships among physiological variables. Data from various sensor nodes is received by a base station or node with more memory and processing power. A dynamic threshold is then used to identify the error and generate alarms using majority vote analysis to identify unusual sensors. In order to predict the sensor value, the established dynamic threshold for error calculation, the established majority voting to determine whether to generate an alarm and the prediction of the value of one sensor at a time based on data history are all applied. Finally, anomalies and error alarms are detected using the dynamic threshold calculation technique and the majority vote, respectively. Between the predicted values and the sensor-provided values, the error computation stage detects a difference greater than the threshold value. The threshold for telling an error warning apart from a genuine warning has been reached. This approach establishes an accuracy threshold value that varies over time by analyzing historical data which raises the cost of computation [17].

In another method data was obtained utilizing mobile data gathering equipment. Each area's mobile data collection machine is in charge of gathering information from the area's cluster head nodes. The anomaly detection algorithm is used by the mobile information machine in place of sensor nodes. The disadvantage of this method is that it relies on a mobile data gathering unit that roams the environment to find abnormal nodes. As a result, some abnormal nodes might not be present and thus go undetected when that portion of the network is being examined. On the other side, due to environmental issues, a machine may be unable to reach the desired sites. Furthermore, this expensive technology cannot immediately defend against attacks because it does not operate online. This strategy is not scalable and effective in networks with lots of sensors [18]. The method of anomaly detection using a mobile data collection system is shown in Figure 1.

In [19] genetic algorithm has been used to generate signature and fuzzy logic to generate rule set for anomaly detection. Generating the signature on each iteration may take a long time. For large networks, the number of rules will be very large. A new fitness function is designed for genetic algorithm (GA) and using artificial neural network (ANN) as a classifier to detect abnormal nodes. In [20] provides an optimal solution by providing an integrated framework that combines the use of a high-cost yet highly accurate detector, called an oracle detector, and a low-cost, low-accuracy detector, called a partial detector. A detection pattern is created and optimized using the first-order approximation method. Simulation results show that combining multiple detectors in an optimal pattern is necessary to provide low execution time overhead.

Anomaly detection is one such area to prevent malicious attacks or reduce errors and noisy data in millions of wireless sensor networks. Outlier detection models should not compromise the quality of data. It should detect anomalies in offline or online mode with accuracy, better performance and minimum network resource consumption. There are various machine learning techniques that have been used by several researchers these days to detect outliers. This paper presents a survey on outlier detection in WSN data using different machine learning techniques [21]. In [22] a distributed online OCSVM is formulated for anomaly detection in networks and the decentralized cost function is obtained. To get a decentralized implementation without transferring the original data, a random approximation function is used to replace the kernel function. Furthermore, to find a suitable

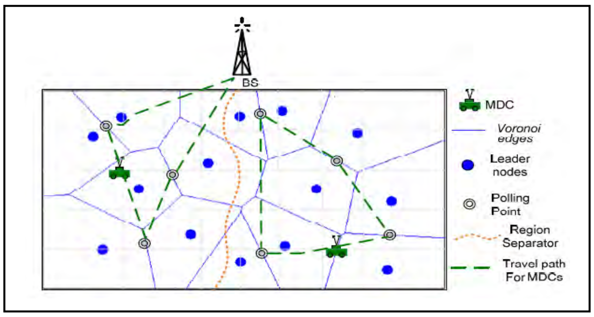

Figure. 1. Detecting anomalies with a mobile data collection machine

approximation dimension, a sparse constraint is added to the decentralized cost function to obtain another one. Then these two cost functions are minimized by stochastic gradient descent and two distributed algorithms are derived.

In [23] for the first time, introduce autoencoder neural networks to WSN to solve the problem of anomaly detection. A two-part algorithm is designed, which is based on the sensors and the cloud of the Internet of Things, respectively, so that (i) anomalies in the sensors can be fully distributed and without the need to communicate with any other sensor or cloud ; identified, and (ii) the relatively more computationally intensive learning task can be performed by the cloud at a much lower (and configurable) frequency. In [24] machine learning-based methods for outlier detection are discussed, among which Bayesian network seems to be advantageous over other methods. Bayesian classification algorithm can be used to calculate the conditional dependency of nodes in WSN. This method can also calculate the amount of missing data.

In [25] an anomaly detection method (STCIE) using spatio-temporal correlation and information entropy is proposed. By exploiting the spatial-temporal relationship of the sensor data, maximum correlation and weighted variation coefficient are introduced. The maximum correlation and weighted coefficient of variation are used to analyze the status of sensor nodes, and the confidence interval method is adopted to realize the adaptive threshold update. To improve the detection accuracy, the abnormal sensor node is confirmed by the linear least square estimation method using information entropy (IE-LLSE). Information entropy is adopted to analyze data fluctuations to achieve the best prediction accuracy. In [26] proposes an anomaly detection algorithm based on mean shift and median absolute deviation (MSAMAD), which detects wormhole attacks by detecting abnormal number of transmissions and abnormal one-hop time between nodes. MSAMAD does not require special hardware and precise time synchronization, and the communication overhead is low. The simulation results show that this method has a higher detection rate than other methods, especially in short-range wormhole attacks.

3. Proposed Method

Clustering is used to find a solution to the issue with the mobile data collection machine technique. The Euclidean distance is used to group the sensor nodes, which are distributed at random in a given area. The network is assumed to have a single hop, and each cluster is given a failing cluster head. Without the aid of middlemen, all nodes can connect directly to the sink node. However, three issues need to be addressed:

a) *Detection of Abnormal Node*

There are abnormal nodes found in the relevant cluster heads. A distinctive identification number is assigned to every node. A threshold is set in order to identify the data. The cluster head analyzes the data from the nodes, and if a node's data is below or above the defined threshold value, it is identified as an anomalous node based on its unit ID and its data is ignored. As a result of the cluster head processing a significant amount of data with a constrained bandwidth, even though we have more sensor nodes than the reference method, the processing volume in the sink does not increase. Figure 2 shows how the cluster head detects node anomalies.

b) *Detection of an abnormal cluster head*

The sink node is in charge of identifying abnormalities in head nodes by comparing the cluster head's current behavior with its previously recorded correct behaviors in the sink, and as a result, the transmitted data is incorrect. The cluster head's sink is also eliminated, and depending on how much energy a failing cluster head uses, it should be replaced. The sink has detected a cluster head anomaly in Figure 3.

c) *Determination of a new cluster head*

In order to avoid selecting the anomalous node as the cluster head after the discovery of cluster head anomalies, specific procedures for selecting the new cluster head based on the amount of energy are taken into account. The first node sends a Hello message to its neighbors to identify the cluster head and asks them for some energy when it discovers a flaw in the cluster head and does not receive a confirmation message from the sink via the cluster head. The mother node resends the cluster head's confirmation message before transmitting it if the majority of nodes approve the cluster head. A new cluster with a new mother node will begin to form if no confirmation message is received. It has a blacklist of abnormal nodes even though not every node from the prior cluster responds to this new request. The sink and cluster head, respectively, are in charge of inspecting for cluster head sensor failure at the cluster head and node levels. The cluster head flags the node as abnormal and removes it from the circuit if a hardware issue is discovered. The cluster head saves the data if a node fails, and the sink node saves the data

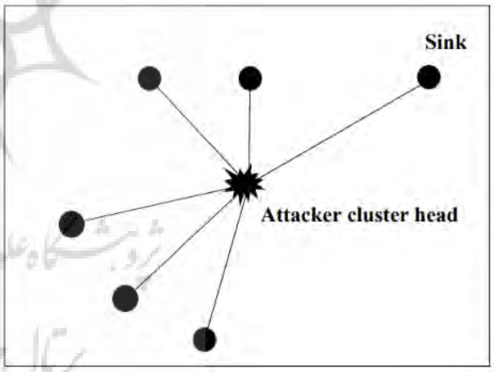

Figure. 2. Detection of node anomaly by cluster head

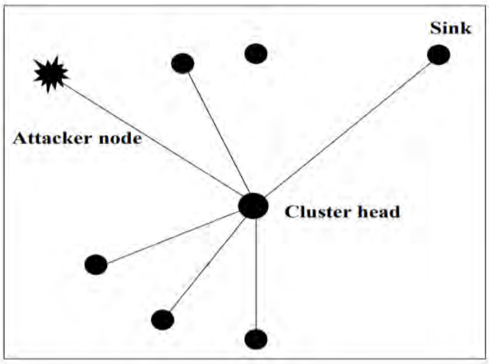

Figure. 3. Detection of cluster head anomaly by the sink

if the cluster head does. If the cluster head fails for any reason, the circuit is broken, and the mother node requests a replacement, which it selects based on the highest level of energy. The new cluster head must report the old cluster head as destructive. Figure 4 displays the cluster head determination algorithm.

4. Simulation of the Proposed Method

Finding the defective sensor is the simulation's goal. Using the Intel Research Laboratory Database, a collection of gathered measurements with deteriorating sensors that is freely accessible, we duplicate the MATLAB software's solution. In terms of their failure model, these sensors manifested as shock pulses that can be detected. It is discovered that the sensor has failed, rendering the data useless. However, this does not imply that the sensor is hostile or bothersome. This work used Euclidean distance to cluster sensors in order to identify bothersome ones. Because we had a database that only revealed failing sensors that deteriorate over time rather than bothersome sensors, we randomly distributed the sensors in this part of the simulation in a 50*50 rectangle space divided into nine equal portions. In Figure 5, Normal and abnormal nodes, as well as cluster head nodes, are represented by +, a circle, a square, and a rhombus, respectively.

Each round of the software's operation identifies abnormal nodes before sending the data from the cluster head to the sink. Since all cluster heads have direct access to the sink and send their data there, the network is viewed as a single hop in this scenario. Several things didn't happen in this simulation, like the cluster head being able to reach all of the nodes. There is still a cluster head in that framework and our clustering structure is unharmed. Our clustering size would have varied if our nodes were more dispersed, followed by the formation of larger or smaller clusters. All nodes are in the same cluster so the range is still good. To do this, a threshold is established to identify aberrant nodes (temperature above 40% and humidity below 18%). The reference article's threshold is chosen for convenience, even though new standards can be created. Depending on the application and signal, there are several simple ways to set a threshold. Anomalies result from the combination of unnatural conditions—in this instance, the ambient temperature is above 40 °C and the humidity is below 18 °C—which are both present. Because there is a link between sensor failure and network performance, an unreliable node for transmitting data is likely to have energy issues.

As a result, in the event of an anomaly, the anomalous node may also be labeled as a bad node, implying that we don't trust the data it sends and that it is unreliable on the network. In light of this assumption and simulation, we seek to confirm that our approach, which plots anomalous nodes and cluster heads and displays clusters with anomalous nodes, is effective. The appropriate cluster head detects the node anomaly in each section. As part of the protocol for locating the anomalous node, a number is added to the counter if the temperature or humidity is greater than or lower than 40. When the node counter reaches two, the node is deemed abnormal. The misbehaving node is depicted as a circle. The cluster head notifies the sink of the node anomaly in subsequent rounds when this node fails to transmit data to it. The sink identifies the anomalous cluster head by comparing the cluster head's present behavior to its previous behavior. To accomplish this, a number of actions are taken. The cluster head sends the average data to the sink after gathering data from each node. The energy of the cluster head is decreased by half a joule for each time the information is transmitted. The cluster leader is believed to have behaved morally and gave the sink the right information every ten rounds during the first ten rounds in which information is sent. The data is compared to the average data from the previous ten rounds, starting with the eleventh round. The cluster head is referred to as an anomalous cluster head if the information is more than twice the average or less. Squares represent the cluster heads, which will be eliminated in subsequent rounds. The new cluster head is chosen as the member with the most energy among the other nodes. Nodes 2, 3, 5, 13, 15, 16, 17, 18, 27, 31, 40, and 54, according to simulation results, have anomalies. As illustrated, the amount

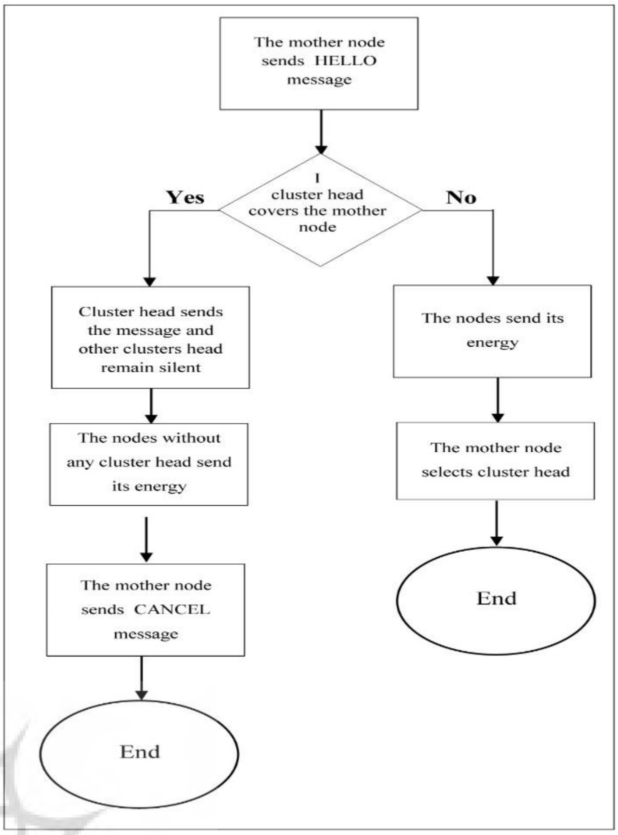
The mother node sends HELLO message
I cluster head covers the mother node
Yes
No
Cluster head sends the message and other clusters head remain silent
The nodes send its energy
The nodes without any cluster head send its energy
The mother node selects cluster head
The mother node sends CANCEL message
End
End

Figure. 4. Cluster head determination algorithm

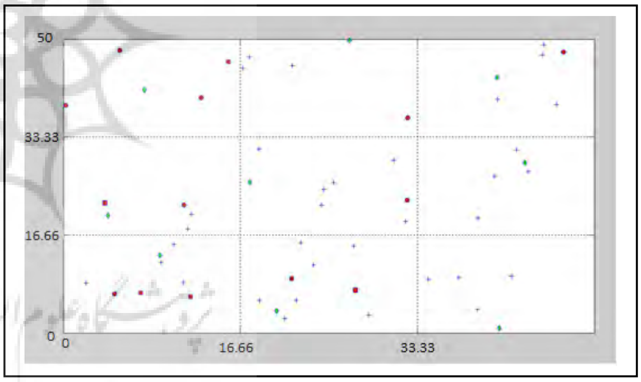

Figure. 5. Normal and abnormal nodes and cluster head

of data sent in the information sending section exceeded or fell below the threshold, causing the node to malfunction. In the humidity diagram, Figure 6 shows a going pulse that represents the anomaly in node 2.

Near the beginning of the diagram, the anomaly can be seen in nodes 3, 16, 18, and 54 as reciprocating pulses. As an illustration, Figure 7 displays the diagram of node 16.

Figure 8 depicts the node 5 anomaly as noise anomalies.

Nodes 15 and 17 have oscillating anomalies, and data transmission is disrupted. Figure 9 displays the node 15 diagram. Even though breaks cannot be referred to as anomalies, there is a connection between them, and the interrupts here show that the entire device has failed.

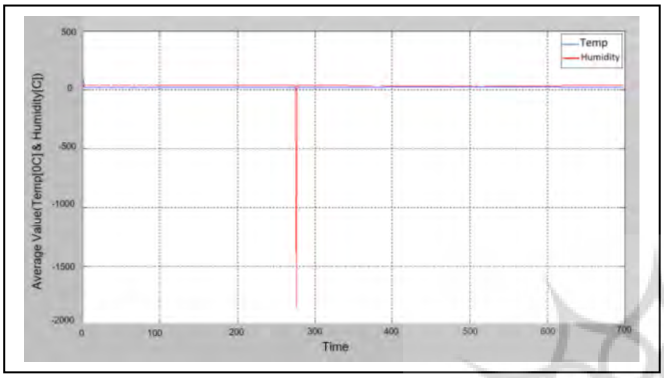

Figure. 6. The anomaly of node 2

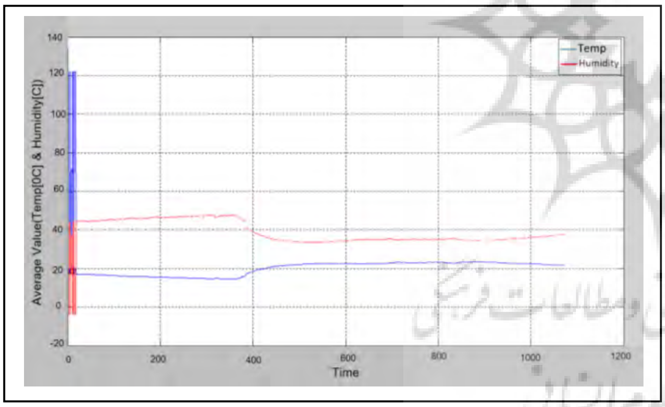

Figure. 7. The anomaly of node 16

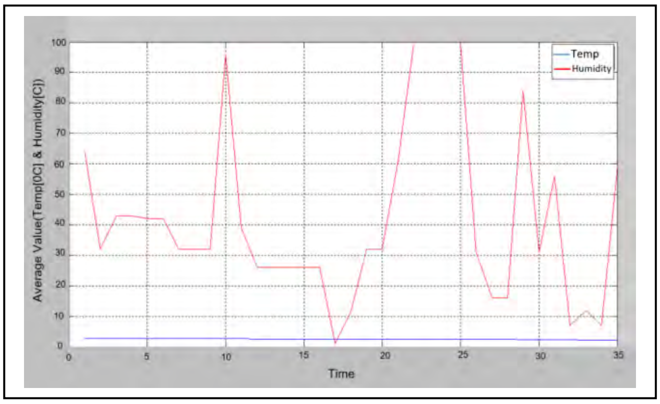

Figure. 8. The anomaly of node 5

Figure 10's anomaly at node 18 shows a sharp rise in which the humidity is constant while the temperature rises quickly.

Node 31 has an anomaly in the form of successive pulses, as shown in Figure 11.

Figure 12 depicts the node 40 anomaly, which appears as oscillating pulses.

5. The Performance Evaluation

The accuracy of our algorithm, which finds anomalies, is based on a number of factors. The comparison criterion should verify that aberrant nodes are found using the threshold and that no nodes with detectable anomalies remain.

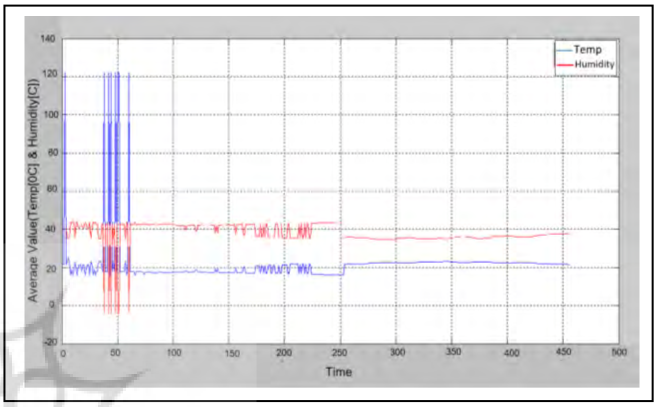

Figure. 9. The anomaly of node 15

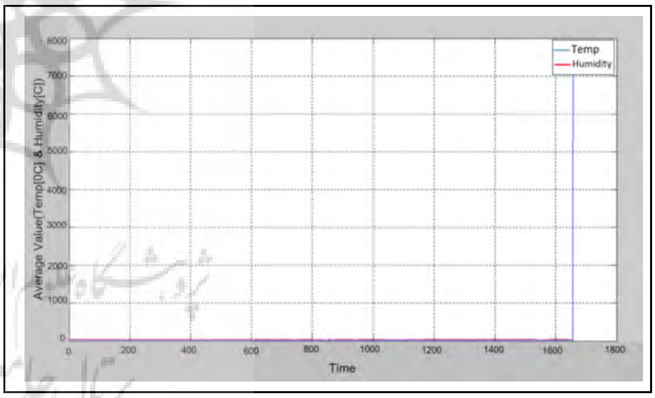

Figure. 10. The anomaly of node 18

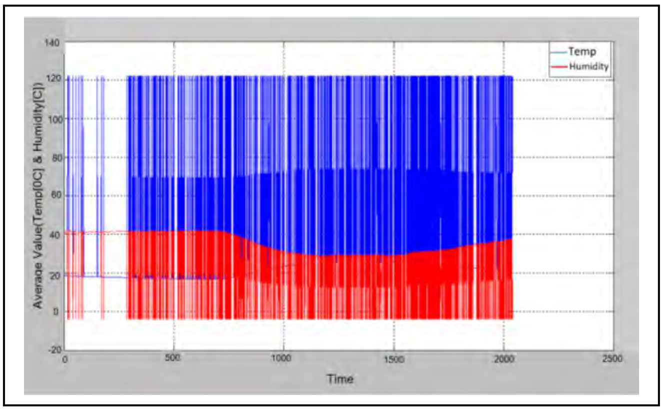

Figure. 11. The anomaly of node 31

Many different types of sensors use this technique and in extremely large dimensions; nevertheless, in terms of data, it is not equivalent to the reference method. Due to the usage of a mobile data gathering unit, the reference technique cannot handle enormous amounts of data. The process used by the robot to collect data is incredibly time-consuming, has a sizable delay, and takes exponentially longer as the number of sensors rises. Additionally, the cost increases exponentially along with the increase in mobile data collection units. It is possible to test more than 57 sensors, but the Intel Laboratory Database only contains 57. In Figure 13, normal and abnormal nodes are represented by a + and a circle, respectively. A square and a rhombus are used to represent aberrant and new cluster head nodes, respectively.

6. ACCURACY DIAGRAM

Figure 14 displays the accuracy diagram. The number of nodes and their corresponding accuracy percentages are displayed on the horizontal and vertical axes, respectively. A node is not regarded as abnormal if its accuracy is 100, which indicates that there have been no errors. If the accuracy is less than 100, an anomaly has occurred in that node, and if the accuracy is lower, the anomaly is more serious. If an abnormality is discovered twice in a node using the proposed method, the node is classified as abnormal. Node 31 has more abnormalities than the other nodes, according to the diagram.

7. Roc Diagram

The effectiveness of the proposed method was shown using a Receiver Operating Characteristic (ROC) diagram in terms of the rate of false positives and detection. The horizontal and vertical axes of the ROC diagram depict a false positive rate and a true positive rate, respectively. The Mahalanobis Distance (MD) method is used to create the ROC diagram. Sensor anomalies are detected using the MD between anticipated and real multivariable instances. System outputs are designated as Positive (P) or Negative (N) in two-tier prediction (binary classification). A "True Positive" is a circumstance where the experiment's outcome matches the prediction of P and the actual results are P. (TP). However, this is referred to as a "False Positive" if the real numbers are N. (FP). When both the predicted and actual values are negative, this situation is referred to as "True Negative" (TN). A prediction result of N when the actual data is P also produces a "False Negative" (FN). Eq.(1) calculates the Detection Rate (DR) as follows:

$$\textit{Detection Rate (True Positive Rate)} = \frac{TP}{FN+TP} \qquad (1)$$

Equivalent (2) can be used to determine the False Positive Rate (FPR) if TP and FP are true and false positive values, respectively.

$$\textit{False Positive Rate} = \frac{FP}{FP+TN} \qquad (2)$$

Figure 15 depicts the relationship between the DR and the false positive rate for the suggested technique using a ROC diagram. A high DR and low false alarm rate are ideal for an anomaly detection system. Figure 15 shows aberrant nodes seen in space. The error value is lower when the graph is higher. In comparison to other nodes, the highest graph is associated to node 3, and it has the least amount of inaccuracy. The lowest graph, on the other hand, belongs to node 31, which has the most inaccuracy.

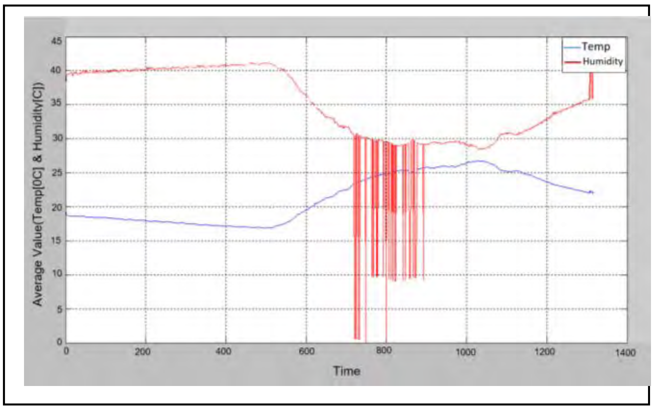

Figure. 12. The anomaly of node 40

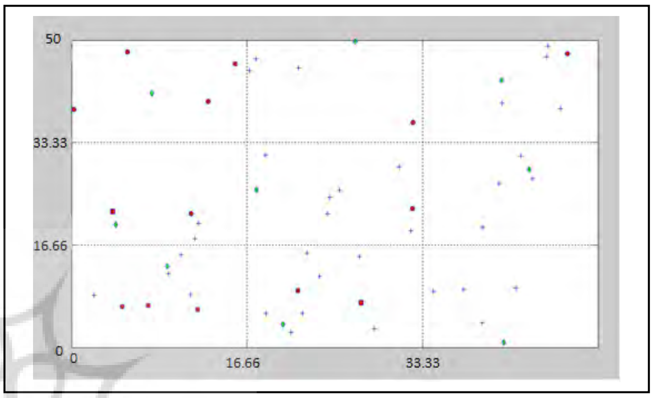

Figure. 13. Detection of node and cluster head anomalies by the proposed method

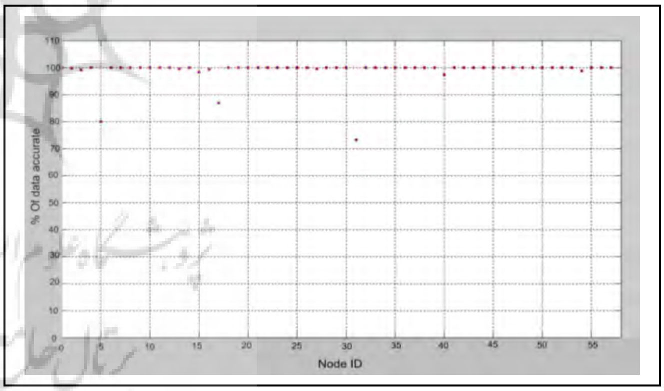

Figure. 14. Accuracy diagram

8. Conclusion

This paper presents a novel approach for clustering-based anomaly detection in WSN nodes. The cluster head and sink node, respectively, were found to have node and cluster head anomalies. The Intel Laboratory Dataset was used to assess the solution's effectiveness, and a threshold was created to detect node anomalies in the cluster head. Furthermore, the cluster head anomaly was discovered based on its previously

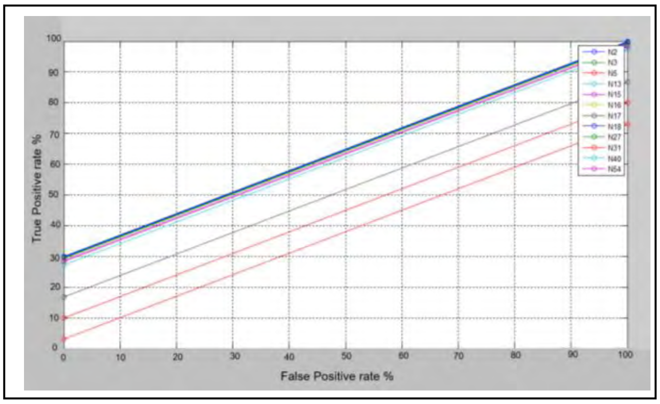

Figure. 15. ROC diagram

documented sink characteristics. The proposed solution has a few advantages over the current method. In this proposed method doesn't need any external circuits or extra resources. However, because of its physical makeup, the data collection apparatus might be duped by questionable nodes. Additionally, as opposed to the data gathering apparatus, the sink node, assumes control of a new node. Our method is online, so it can quickly fend off threats. Our main contribution is the development of a novel approach for identifying intrusive nodes in WSNs by employing clustering. Our proposed method can improve efficiency, scalability, and online specificity.

9. Future Works

In this paper, a solution has been developed to detect abnormal nodes and cluster heads in wireless sensor networks for single-step networks, where all nodes have direct and immediate relationship with the sink. This method can be generalized for multi-step networks.

Declarations

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

Authors' contributions

SG: Study design, acquisition of data, interpretation of the results, statistical analysis, drafting the manuscript; RB: Study design, interpretation of the results.

Conflict of interest

The authors declare that there is no conflict of interest.

References

[1] Q. E. K. Mamun, "Constraint-Minimizing Logical Topology for Wireless Sensor Networks," Doctoral dissertation, *Clayton School of Information Technology Monash University*, vol. 2, no. 11, pp. 400-413, 2011.

[2] M. Elhoseny, H. Elminir, and Ai M. Riad, "Recent Advances of Secure Clustering Protocols in Wireless Sensor Networks," *International Journal of Computer Networks and Communications Security*, 2014.

[3] J. Y. Yu, E. Lee, S. R. Oh, Y. D. Seo, and Y. G. Kim, "A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security," *IEEE Access*, vol. 8, pp. 45304-45324, 2020.

[4] YuZhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6-28, 2008.

[5] R. Wu, Xi Deng, RDLu, and XoShen, "Trust-based anomaly detection in wireless sensor networks," *1st IEEE International Conference on Communications in China, ICCC*, IEEE, 2012, pp. 203-207.

[6] R. Jyothi, and N. G. Cholli, "New Approach to Secure Cluster Heads in Wireless Sensor Networks," *5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, IEEE, 2019, pp. 1097-1101.

[7] Z. W. Hussien, D. S. Qawasmeh, and M. Shurman, "MSCLP: Multi-Sinks Cluster-Based Location Privacy Protection scheme in WSNs for IoT," *32nd International Conference on Microelectronics (ICM)*, IEEE, 2020, pp. 1-4.

[8] N. Berjab, H. H. Le, C. M. Yu, S. Y. Kuo, and H. Yokota, "Abnormal-Node Detection Based on Spatio-Temporal and Multivariate-Attribute Correlation in Wireless Sensor Networks,". *IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, IEEE, 2018, pp. 568-575.

[9] N. Berjab, H. H. Le, and H. Yokota, "A Spatiotemporal and Multivariate Attribute Correlation Extraction Scheme for Detecting Abnormal Nodes in WSNs," *IEEE Access*, vol. *9*, pp. *135266-135284*, 2021,

[10] R. Kumar, and P. Rajpoot, "Optimized H-LEACH algorithm for clustering to improve lifetime of WSN," *3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, IEEE, 2018, pp. 2393-2398.

[11] N. Khalil, M. R. Abid, D. Benhaddou, M. Gerndt, "Wireless sensors networks for Internet of Things," *IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) Symposium on Public Internet of Things*, IEEE, 2014, pp.1-6.

[12] A. Al-Riyami, N. Zhang, and J. Keane, "An adaptive early node compromise detection scheme for hierarchical WSNs," *IEEE Access*, vol. 4, pp. 4183-4206, 2016.

[13] N. Wang, and J. Li, "Shortest path routing with risk control for compromised wireless sensor networks," *IEEE Access*, vol. 7, pp. 19303-19311, 2019.

[14] S. Cao, Q. Wang, Y. Yuan, and J. Yu, "Anomaly Event Detection Method Based on Compressive Sensing and Iteration in Wireless Sensor Networks," *Journal of Networks*, vol. 9, no. 3, p. 711, 2014.

[15] H. E. Egilmez, and A. Ortega, "Spectral Anomaly Detection Using Graph-Based Filtering for Wireless Sensor Networks," *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, IEEE, 2014, pp. 1085-1089.

[16] S. A. Haque, S. M. Aziz, and M. Rahman, "Sensor Anomaly Detection in Wireless Sensor Networks for Healthcar," *National Center for Biotechnology Information*, 2015.

[17] R. Ahmad, E. A. Sundararajan, and T. Abu-Ain, "Analysis the Effect of Clustering and Lightweight Encryption Approaches on WSNs Lifetime," *International Conference on Electrical Engineering and Informatics (ICEEI)*, IEEE, 2021, pp. 1-6.

[18] Quazi Mamun, Mohammed Kaosar, Md Rafiqul Islam, "Anomaly Detection in Wireless Sensor Network," *in Journal of Networks*, vol. 10, no. 4, p. 217415, 2014.

[19] Rana Jafri; Rakesh Kumar, "Outlier Detection in WSN," *3rd International Conference on Inventive Computation Technologies (ICICT)*, 2018.

[20] Muhammad Alfian Amrizal; Luis Guillen; Takuo Suganuma, "Toward an Optimal Anomaly Detection Pattern in Wireless Sensor Networks," *IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, 2019.

[21] Rajendra Kumar Dwivedi; Arun Kumar Rai; Rakesh Kumar, "A Study on Machine Learning Based Anomaly Detection Approaches in Wireless Sensor Network," *10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2020.

[22] Xuedan Miao; Ying Liu; Haiquan Zhao; Chunguang Li, "Distributed Online One-Class Support Vector Machine for Anomaly Detection Over Networks," *IEEE Transactions on Cybernetics*, 2019.

[23] Tie Luo; Sai G. Nagarajan, "Distributed Anomaly Detection Using Autoencoder Neural Networks in WSN for IoT," *IEEE International Conference on Communications (ICC)*, 2018.

[24] Rajendra Kumar Dwivedi; Sonali Pandey; Rakesh Kumar, “A Study on Machine Learning Approaches for Outlier Detection in Wireless Sensor Network,” *8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2018.

[25] Lingqiang Chen; Li Xu; Guanghui Li, “Anomaly Detection Using Spatio-Temporal Correlation and Information Entropy in Wireless Sensor Networks,” *International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, 2020.

[26] Yihan Sun; Yunli Chen, “Detection of Wormhole Attacks in Wireless Sensor Networks Based on Anomaly Detection Algorithms,” *2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, 2022.

Sara Gorgbandi received the Bachelor's degree in Electrical-Electronic Engineering from Tuysarkan Azad University, Hamedan from 2005 to 2009. She received the Master's degree in information and communication technology engineering from Tehran University of Science and Technology from 2011 to 2015. She was representative of Nadco company in Arak from 2009 to 2015. She is data and switch expert of the General Department of Communication Infrastructure of Central Province from 2010 until now. She is working on Logic circuit training circuits using FPGA and VHDL language and She is interested in telecommunication networks and robotics.

Dr. Reza Berangi has (PhD) in Mobile Telecommunications from Victoria University of Technology, Melbourne, Australia, 1998. He received MS., Electronic Engineering, Iran University of Science and Technology, Tehran, Iran, 1989. He received BSc, Telecommunication Engineering, Iran University of Science and Technology, Tehran, Iran, 1985. He is Associate Professor, Faculty of Computer Engineering, Iran University of Science and Technology, Since Sept 2001. He was Research Fellow, Electrical Engineering Dept, Victoria University of Technology, Australia, 1997-2001. He was Sessional tutor, Electrical Engineering Dept, Melbourne University, Australia, 1994-1997. He was Sessional tutor, Electrical Engineering Dept, Victoria University of Technology, Australia, 1993-1997. He was Research staff, Jahad Daneshgahi, Iran University of Science and Technology,1979-1992.