International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6690
***Article Received**: 06 March 2023 **Revised**: 22 April 2023 **Accepted**: 07 May 2023*

Outlier Detection Mechanism for Ensuring Availability in Wireless Mobile Networks Anomaly Detection

Allen Paul L.Esteban[1], Alexander Cochanco[2], Jet Aquino[3], Rolaida Sonza[4]
[1]MSIT Faculty, Graduate School Department,
Nueva Ecija University of Science and Technology,
Philippines.
estebanallenpaul@gmail.com
[2]Faculty, Information Technology Department,
Nueva Ecija University of Science and Technology,
Philippines.
alexander.cochanco@neust.edu.ph
[3]Faculty, Graduate School Department,
Nueva Ecija University of Science and Technology,
Philippines.
jetaquino.neust@gmail.com
[4]Faculty, Graduate School Department,
Nueva Ecija University of Science and Technology,
Philippines.
rolaidasonza@gmail.com

Abstract: Finding things that are significantly different from, incomparable with, and inconsistent with the majority of data in many domains is the focus of the important research problem of anomaly detection. A noteworthy research problem has recently been illuminated by the explosion of data that has been gathered. This offers brand-new opportunities as well as difficulties for anomaly detection research. The analysis and monitoring of data connected to network traffic, weblogs, medical domains, financial transactions, transportation domains, and many more are just a few of the areas in which anomaly detection is useful. An important part of assessing the effectiveness of mobile ad hoc networks (MANET) is anomaly detection. Due to difficulties in the associated protocols, MANET has become a popular study topic in recent years. No matter where they are geographically located, users can connect to a dynamic infrastructure using MANETs. Small, powerful, and affordable devices enable MANETs to self-organize and expand quickly. By an outlier detection approach, the proposed work provides cryptographic property and availability for an RFID-WSN integrated network with node counts ranging from 500 to 5000. The detection ratio and anomaly scores are used to measure the system's resistance to outliers. The suggested method uses anomaly scores to identify outliers and provide defence against DoS attacks. The suggested method uses anomaly scores to identify outliers and provide protection from DoS attacks. The proposed method has been shown to detect intruders in a matter of milliseconds without interfering with authorised users' privileges. Throughput is improved by at least 6.8% using the suggested protocol, while Packet Delivery Ratio (PDR) is improved by at least 9.2% and by as much as 21.5%.

Keywords: Anomaly detection, MANET, RFID-WSN, DoS.

I. Introduction

One of the often-studied topics that have drawn the interest of numerous fields, including medicine, image processing, finance, insurance, wireless networking, MANETs, etc. is anomaly detection. Security is a significant issue that needs to be further addressed, and research studies and other written works offer numerous answers to this problem. One of the key ones for MANET is security through outlier detection [1]. To provide a more secure environment, prevention and outlier detection work in tandem. A few of the widely used protocols are included in hybrid techniques that are created. The QoS, energy optimization, and system performance of the system are impacted by the detection of outliers utilizing a hybrid framework that employs various data mining or machine learning methods [2].

No matter where they are geographically located, users can connect to a dynamic infrastructure using MANETs. Small, powerful, and affordable devices enable MANETs to self-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6690
***Article Received**: 06 March 2023 **Revised**: 22 April 2023 **Accepted**: 07 May 2023*

organize and expand quickly. These devices have the ability to recognize other devices and put the necessary organization in place to allow for communication and the sharing of services and data. In decentralized MANETs, nodes are responsible for message delivery and network management. The changing topology of MANET causes a number of problems with message routing [3]. When compared to wired networks, MANETs are more susceptible to malicious attacks due to mobile nodes, risks from compromised nodes within the network, limited security, dynamic topology, scalability, and the absence of centralized management. Anomalies in MANET that impact throughput, packet delivery, connection capacity, energy consumption, end-to-end delay, etc. must be addressed. In addition to the explicit needs of the MANET, such as energy, route stability, resource estimate, etc., the QoS requirements that MANETs should address include bit rate error, route length, delay, bandwidth, etc. If possible, an ideal path is chosen and resources are kept in reserve along the way [4].

Wireless networks called MANETs are made up of autonomous nodes that constantly move around and organize themselves haphazardly. With MANETs, the network topology is constantly shifting in an unpredictable manner. MANETs can be used in a variety of settings, including military operations, home networks, mobile conferencing, and disaster relief. A basic MANET's wireless nodes are joined together without a static infrastructure and communicate by sending data packets [5]. Due to a number of reasons, including changeable topology, wireless node communication, and a lack of appropriate methods for communication management and control, MANETs are vulnerable to assaults. As a result, there are numerous difficult problems with MANETs that need to be solved. The main issues that MANET must address include the lack of centralized control, a lack of resources, changeable topology, and network dimensions. Other concerns that need to be solved include the lack of a borderline, scalability, a limited supply of electricity, and different performance problems including bandwidth availability. Adequate performance and secure connectivity between nodes are difficult to achieve [6].

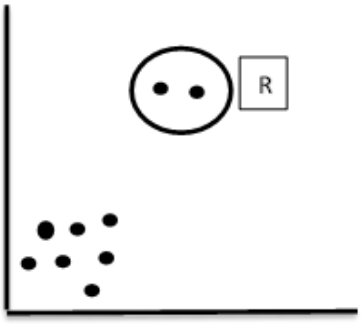

Figure I: Global Outlier points in region R.

Outliers are trends that differ from what is typically expected to occur, as indicated. Despite the fact that this strategy seems straightforward, it is undoubtedly a very difficult assignment for the reasons listed below. The work of defining a normal zone in an outlier detection mechanism is difficult since the boundaries between normal and abnormal objects are often thin, making it difficult to compute all conceivable normal items or objects in a dataset [7]. For the items that are close to the borders, there is a chance that an outlier will be mistaken for a regular object, and vice versa. Also, it is difficult to access the labeled data for the training procedure. MANETs are among the domains where outlier identification is frequently used. Because of their dynamic nature, MANETs are vulnerable to a variety of security risks, making the development of adaptive security techniques difficult in these situations. From this vantage point, anomaly-based intrusion detection systems are useful for defending networks from malicious attacks. A few hurdles must be overcome in order to use outlier detection in MANETs for intrusion detection and improve security and performance [8].

1. In order to enable secure communication in MANETs, attack signatures must be kept through a distributed technique because there is no central or reliable supervisory node.

2. Robustness and highly dynamic network topology enhance the likelihood that routing tables will need to be generated and modified repeatedly, which requires more energy and requires sending more packets, increasing overhead.

3. Security is a serious issue because MANETs are open networks with no clearly defined boundaries. A coordinated detection system must be used for the identification and defense against serious threats in order to incorporate security.

4. In order to counter new and varied threats, it is necessary to create and apply protocols that can be roughly divided into proactive, reactive, and hybrid categories. For resource-constrained networks that can produce the best results, more advanced protocols, and simpler methods must be developed.

5. Because the mobile sensor devices that makeup MANETs have limited memory and poor computational power, the network only offers a small amount of bandwidth. A MANET anomaly detection system necessitates a high bandwidth exchange of condensed traffic among nodes [9-10].

II. Related work done:

A key task in many applications, including criminal activity, e-business, credit card fraud detection, many medical sectors, intrusion detection, etc., is extracting information from vast amounts of data. In contrast to the outcomes of traditional data mining techniques, which focus on discovering patterns

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6690
***Article Received**: 06 March 2023 **Revised**: 22 April 2023 **Accepted**: 07 May 2023*

that frequently occur in the data, anomaly detection approaches prioritize pattern determination that arises sporadically in the data [11]. As the line between normal from abnormal items is so thin, it is challenging to calculate all the likely normal behaviour in a dataset connected to a particular application. It is challenging to distinguish between an anomaly and a typical thing, and vice versa, because there is no clear border.

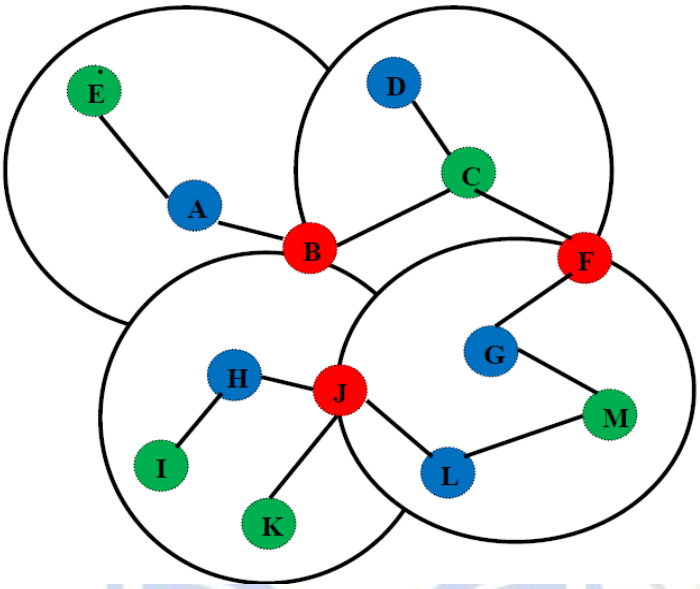

Figure II: Route establishment procedure in MANETs [Google].

Care must be used while choosing a distance measurement between the objects [12]. Also, the applications for which it must be used must be taken into account in order to model the relationship between the items. A small deviation, for example, is considered an anomaly in a dataset connected to the healthcare industry, yet larger variations are considered anomalous in a dataset related to marketing. Anomaly detection is a crucial task during setup in Mobile Ad Hoc Networks (MANETs). Several currently used protocols and services for MANETs reflect a compliant network environment and do not prioritize security as a top priority. As a result, anomaly detection is essential to MANETs since it serves as the second line of defence for high-security needs [13].

In the past, statistical methods were used to detect outliers. A probability distribution is evaluated in statistical methods for two reasons. One is used to gather data dissemination, while the other estimates data occurrences in order to evaluate the model's fitness. Other studies have utilized non-Gaussian-based parametric statistical-based approaches, non-Gaussian-based parametric statistical-based approaches, and a few more studies have employed non-parametric statistical-based approaches [14]. Some researchers have proposed a two-level method for locating distant sensors. The spatial correlation of the current measurement is used among nearby sensor nodes to distinguish between outlying sensors and event boundaries. The difference between the median reading and the particular reading of the neighbour is calculated for each node. The node is classified as an outlier if the difference exceeds the first selected threshold and as an inlier otherwise [15].

In the studies conducted by a few academics, spatiotemporal correlation data from the sensor is used to detect an outlier. In another research study, a non-Gaussian parametric technique is applied. It uses sensor data for operations like maximum, average, etc., and spatiotemporal correlation. A few scientists employ non-parametric statistical methods for outlier detection in their work [16]. The approach suggested in a few additional research is based on the histogram, while a few authors' proposed work makes use of the kernel function. Authors have suggested a histogram-based method for locating global outliers in sensor network data correlation applications [17]. It is reasonably cheaper to communicate by gathering histogram data. Nevertheless, in a few older methods, the histogram data is not collected for centralized processing; as a result, there is a larger network connection cost. This method can only be used with one-dimensional data and cannot be used with multi-dimensional data [18].

The researchers in the paper suggest a clustering-based outlier identification method for wireless sensor networks. Prior to connecting with other nodes, this method groups the sensor readings into clusters and then combines various clusters [19]. Comparing it to a few other previously suggested ways, it is demonstrated that the communication overhead is smaller. Moreover, this method does not require prior knowledge of the distribution of the data. As a result, this

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6690
***Article Received**: 06 March 2023 **Revised**: 22 April 2023 **Accepted**: 07 May 2023*

method can be applied to an incremental model, which was not the primary goal of the preceding methods. In another article, the same authors offered a classification-based strategy [20]. The method described used a one-class quarter-sphere state vector mechanism in which sensor data that are outlier is regarded to be beyond the quarter sphere. By using this approach, communication overhead is minimized and local outlier identification at each node is achieved. Another classification-based outlier identification method in wireless sensor networks is suggested in the investigations of numerous academics. It makes use of a Bayesian network to isolate local outliers in sensor data streams [21-22].

In a study, the nearest neighbour method was suggested for locating global outliers in wireless sensor networks. Among nearby nodes, a collection of representative data transfers demonstrates the reduction in communication. Each node uses similarity to determine the outlier's distance locally [23]. A broadcast of the identified outliers is sent to the nearby nodes for verification reasons. Since it doesn't use any network structures, the methodology given in was not well suited for a large-scale network. By adopting the form of the aggregate tree, the work given by a select group of academics addresses the shortcomings of earlier work [24]. The technique given in this study prevents broadcasting to each node, demonstrating that the communication cost is significantly reduced. Each node in the tree delivers only the useful portions of the whole data rather than the entire amount, and this process is repeated until the sink has calculated the agreement on the overall results [25].

III. Purpose of the work

1) To research outlier detection methods for the detection of outliers via anomaly score for network defence against DoS assaults.
2) To guarantee availability and cryptographic properties via a MANET outlier detection technique.

IV. The Projected Algorithm:

The methods provided in the study report to guarantee availability, reduce anomaly score inaccuracy, and spot outliers are described in depth here. The anomaly score and standard deviation are computed. The anomaly score is an estimate of the interval value within which the proportional difference between two measurements lies, and it is calculated using the Limit of Agreement (LoA). In the work being proposed, an anomaly score is considered valid if and only if the bounds of agreement are small. In order to determine an anomaly score with a minimal error probability, the simulated annealing method is utilised. Choosing the least error probability between observed and anticipated values yields the optimum value for the nearby anomaly score. In summary, when the likelihood of an incorrect actual result is less than the likelihood of an incorrect forecast result, an adjacent point is chosen (represented by an anomaly score). The complete simulation time is split into n-slots, and outlier nodes are discovered beginning with the second slot for outlier detection via anomaly score. Together, active and passive nodes help find these anomalous hubs. If a passive node continues to send outbound messages after a certain threshold is reached, it is classified as a bad actor. The process for identifying anomalies ensures the availability property. If a node deviates from the norm beyond the edge conditions, it is considered an outlier.

The process for identifying anomalies ensures the availability property. If a node deviates from the norm beyond the edge conditions, it is considered an outlier. In this study, we use a metric called the anomaly score to single out active nodes that deviate from the norm.

$$Anomaly\ Score = \frac{Total\ (A) - Avg\ (A+P)}{STDEV\ (A)} \pm STDERR \quad (1)$$

$$STDERR = \sqrt{\frac{S^2}{N}} \quad (2)$$

Where, S is the standard deviation of the differences and N represents the sample size used to identify outliers.

Also, the Limits of Agreement (LoA) are taken into account while calculating an anomaly score. The proportional difference between two measurements is estimated as an interval value. This contract's maximum is determined using the following formula:

$$LOA = SE(\text{SystematicError}) + RE\ (Random\ Error) \quad (3)$$

When the same experimental conditions are used again, Systematic Error (SE) occurs in the suggested outlier detection method. Using this method, the anomaly estimation interval is chosen using SE. The 100 ms timeframe is used for the anomaly score calculation. Errors in both the number of outliers and the range of anomaly scores are examples of Systematic Error (SE). Parameters such as Insufficient Calibration Error (ICE), Quantity Error (QE), and Drift Error (DE) are included in both types of SE.

$$SE = ICE + QE + DE \quad (4)$$

Here, ICE takes into account things like the distance between nodes, the numerical models used in experiments, the physical law used to calculate node movement, and any errors introduced by ambient circumstances (temperature, pressure, etc.). When the number of nodes expands, QE integrates the constant value contributed to systematic error. Of fact, adding more nodes to a given area increases the load on adjacent infrastructure, which in turn increases the possibility of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6690
***Article Received**: 06 March 2023 **Revised**: 22 April 2023 **Accepted**: 07 May 2023*

mistakes being made. For the sake of this work, it is assumed to be constant as the addition of more nodes to a network results in a constant but variable amount of initial overhead while the level of error increases proportionally. While computing constant values in the context of experimentation, which can veer in any direction, DE integrates diversity in patterns. For instance, resetting the analysis is preferable for accuracy if the sum of packets sent from nodes does not equal the number of times nodes are classified as source nodes. Variables beyond our control, such as a node's unexpected failure, a black hole assault, or our own overzealous attempts to regulate node behaviour, all contribute to Random Error (RE).

Source, destination, intermediate, sleep, dead, live, idle, undefined, active, and passive nodes are indicated by the letters S, D, I, SL, DN, LN, IN, U, A, and P respectively. The threshold anomaly score is set experimentally and is determined during implementation.

The plan is to segment the simulation period into n time intervals, calculate an anomaly score at the end of each slot (beginning with the second), and then use that score to tally up the number of outliers and inliers at the end of each slot.

Step 1: Determine the set of dynamic nodes (A= [S, D, I]) and the set of static nodes (P= [U]).

Step 2: Split the overall simulation duration into n equal intervals.

Step 3: Make iteration = 1

Step 4: Outlier list =NULL

Step 5: Throughout the iteration of n times, the following are carried out:

Step 6: if iteration equals one,

Step 7: tally up all the A and A+P nodes.

Step 8: If the condition is not met, continue to iterate until the condition is met.

Step 9. Figure out Standard deviation (STDEV) of A utilising (iteration-1)th and iterationth slots, anomaly score, and sum of A and P nodes.

Step 10. Display the node-specific anomaly scores.

Step 11. Add to Outlier list the nodes whose anomaly score is significantly higher than the set threshold.

Step 12. For node in Outlier list

Step 13. Network node discarding as communication method number thirteen

Step 14. Exit for

Step 15. Using the formula iteration+1

Step 16. The Finale

Step 17. The Outlier list nodes should be added to the training dataset along with their characteristics.

V. Result and Discussion:

Throughput and packet delivery rate (PDR) for different nodes in the presence and absence of outliers are analysed and compared with the current method. Since the maximum number of nodes are taking part in the activities of the network, it is determined that the throughput improves with an increase in the number of nodes. The suggested network scenario has throughput within the threshold limits while there are no outliers, and throughput below the lower worthy threshold limit when there are outliers.

5.1. PDR (Packet delivery ratio): PDR is the ratio of packets received to packets sent. The primary success of wireless networks is the transmission of packets. As far as PDR is concerned, this delivery ratio is a success.

$$PDR = \frac{Recieved\ Packet\ Count}{Delivered\ Packet\ Count} \quad (5)$$

5.2. Throughput: The throughput is the rate at which data packets are successfully relayed from the sending node to the receiving node.

$$Throughput = \frac{Forwaded\ data}{Transmission\ time} \quad (6)$$

Table I: Comparative analysis of throughput comparison with and without the presence of outlier nodes

S. No.	Node Count	Throughput (Without outlier)	Throughput (With outlier)	Throughput threshold (Lower)	Throughput threshold (Upper)
1	500	58000	26000	24000	58000
2	1000	62000	41000	58000	62000
3	2000	65000	43000	61000	64000
4	4000	80000	81000	80000	81000
5	5000	92000	94000	90000	140000

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6690
***Article Received**: 06 March 2023 **Revised**: 22 April 2023 **Accepted**: 07 May 2023*

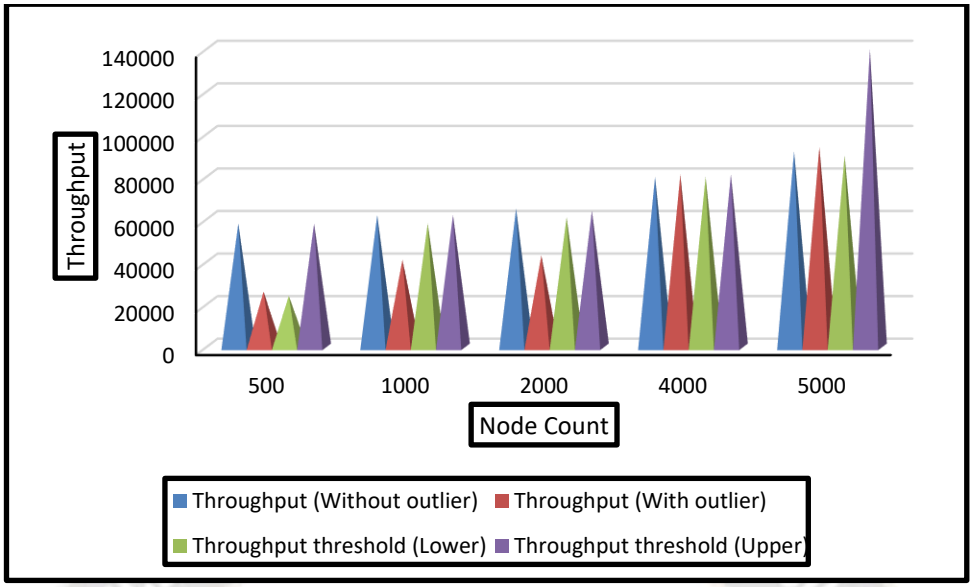

Figure I: Comparative analysis of throughput comparison with and without the presence of outlier nodes

Table II: Comparative analysis of packet delivery rate (PDR) with and without the presence of outlier nodes.

S. No.	Node Count	PDR (%) (Without outlier)	PDR (%) (With outlier)	PDR (%) (Lower)	PDR (%) (Upper)
1	500	89	72	81	95
2	1000	94	73	72	94
3	2000	84	75	83	82
4	4000	95	78	94	99
5	5000	93	81	82	97

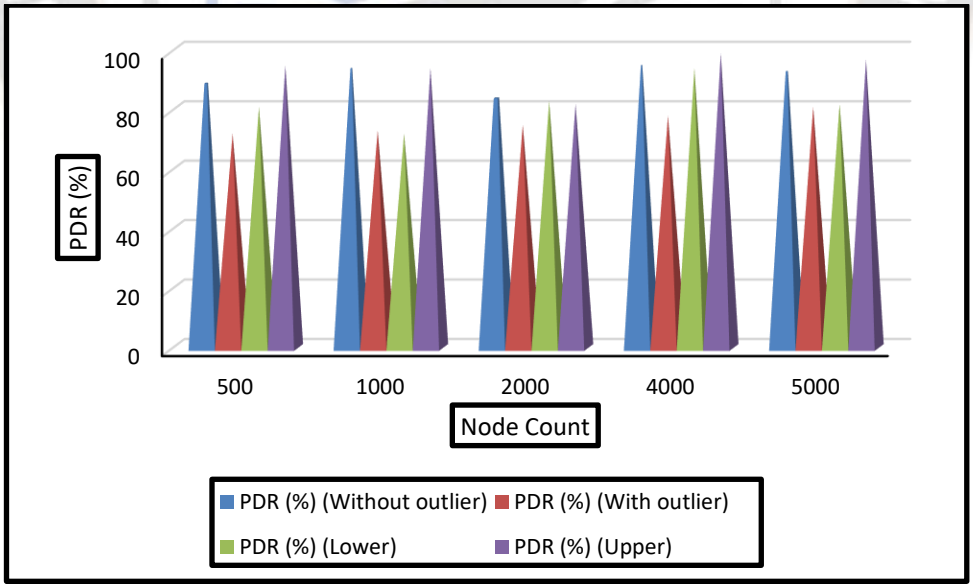

Figure II: Comparative analysis of packet delivery rate (PDR) with and without the presence of outlier nodes.

As a result, if a cluster of nodes is displaying below a specified threshold, it is labelled as an outlier. In addition, a comparison of PDR percentages was performed. The results show that for networks free of outliers, the PDR percentage is within the allowable range, whereas in networks containing outliers, it is below the minimum allowable value. Hence, nodes are deemed to be anomalous if they belong to a group whose PDR falls below some minimum threshold. The results demonstrate that the proposed technique improves both PDR and throughput.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6690
***Article Received**: 06 March 2023 **Revised**: 22 April 2023 **Accepted**: 07 May 2023*

VI. Conclusion:

While there has been a lot of work done on the topic of outlier detection in MANET, persistent and serious problems like security breaches and performance dips persist. There is a need to develop strategies and approaches to help networks be more secure and robust due to the wide variety of security and performance challenges. For anomaly identification in MANET, a hybrid technique is essential. This approach employs an outlier detection mechanism to guarantee the availability of a cryptographically secure RFID-WSN hybrid network with any number of nodes from 500 to 5000. The detection ratio and anomaly scores are used to put the system through its paces against anomalous data. Standard error and anomaly scores were determined. The estimated interval value within which the proportional difference between two measurements lies was calculated using the Limit of Agreement (LoA) for the anomaly score. In the work being proposed, an anomaly score is considered valid if and only if the bounds of agreement are small. To prevent Denial-of-Service (DoS) assaults, the suggested method uses anomaly scores to single out abnormal behaviour. The proposed method has been shown to detect intruders in a matter of milliseconds without interfering with authorised users' privileges. Throughput is improved by at least 6.8% using the suggested protocol, while Packet Delivery Ratio (PDR) is improved by at least 9.2% and by as much as 21.5%.

To better detect new forms of intrusion, future research may wish to facilitate a defence mechanism that learns from past mistakes. MANETs rely heavily on the creation and implementation of network security policies, which presents another topic for investigation. Furthermore, it would be fascinating to explore this strategy to other relevant sorts of applications and assess it in a real-world setting.

Conflict of Interests:

The authors declare that there is no conflict of interests regarding the publication of this paper.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] M. Marimuthu and I. Krishnamurthi, “Enhanced OLSR for defense against DOS attack in ad hoc networks,” J. Commun. Networks, vol. 15, no. 1, pp. 31–37, Feb. 2013.

[2] S. S. Rajput and M. C. Trivedi, “Securing zone routing protocol in MANET using authentication technique,” Proc. - 2014 6th Int. Conf. Comput. Intell. Commun. Networks, CICN 2014, pp. 872–877, 2014.

[3] S. A. Selvi and A. Vijayaraj, “Increasing quality of service in video traffic using zone routing protocol in wireless networks,” in 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), 2016, pp. 1–5.

[4] Chettri L., Bera R. A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. IEEE Internet Things J. 2020;7:16–32. doi: 10.1109/JIOT.2019.2948888.

[5] Andrews J.G., Buzzi S., Choi W., Hanly S.V., Lozano A., Soong A.C.K., Zhang J.C. What Will 5G Be? IEEE J. Sel. Areas Commun. 2014; 32:1065–1082. doi: 10.1109/JSAC.2014.2328098.

[6] Imran A., Zoha A., Abu-Dayya A. Challenges in 5G: How to empower SON with big data for enabling 5G. IEEE Netw. 2014; 28:27–33. doi: 10.1109/MNET.2014.6963801.

[7] Valastro G.C., Panno D., Riolo S. A SDN/NFV based C-RAN architecture for 5G Mobile Networks; Proceedings of the 2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT); Tangier, Morocco. 20–22 June 2018; pp. 1–8.

[8] Asghar A., Farooq H., Imran A. Self-Healing in Emerging Cellular Networks: Review, Challenges, and Research Directions. IEEE Commun. Tutor. 2018; 20:1682–1709. doi: 10.1109/COMST.2018.2825786.

[9] Li R., Zhao Z., Zhou X., Ding G., Chen Y., Wang Z., Zhang H. Intelligent 5G: When Cellular Networks Meet Artificial Intelligence. IEEE Wirel. Commun. 2017; 24:175–183. doi: 10.1109/MWC.2017.1600304WC.

[10] Wu J., Lee P.P.C., Li Q., Pan L., Zhang J. CellPAD: Detecting Performance Anomalies in Cellular Networks via Regression Analysis; Proceedings of the 2018 IFIP Networking Conference (IFIP Networking) and Workshops; Zurich, Switzerland. 14–16 May 2018; pp. 1–9.

[11] Wang M., Handurukande S. A Streaming Data Anomaly Detection Analytic Engine for Mobile Network Management; Proceedings of the 2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress; Toulouse, France. 18–21 July 2016; pp. 722–729.

[12] Song R., Liu F. Real-time anomaly traffic monitoring based on dynamic k-NN cumulative-distance abnormal detection algorithm; Proceedings of the 2014 IEEE 3rd International Conference on Cloud Computing and Intelligence Systems; Shenzhen, China. 27–29 November 2014; pp. 187–192.

[13] Muñoz P., Barco R., Serrano I., Gómez-Andrades A. Correlation-Based Time-Series Analysis for Cell Degradation Detection in SON. IEEE Commun. Lett. 2016; 20:396–399. doi: 10.1109/LCOMM.2016.2516004.

[14] Ibidunmoye O., Rezaie A., Elmroth E. Adaptive Anomaly Detection in Performance Metric Streams. IEEE Trans. Netw. Serv. Manag. 2018; 15:217–231. doi: 10.1109/TNSM.2017.2750906.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6690
Article Received: 06 March 2023 Revised: 22 April 2023 Accepted: 07 May 2023

[15] Alam M.R., Gerostathopoulos I., Prehofer C., Attanasi A., Bures T. A Framework for Tunable Anomaly Detection; Proceedings of the 2019 IEEE International Conference on Software Architecture (ICSA); Hamburg, Germany. 25–29 March 2019; pp. 201–210.

[16] Hussain B., Du Q., Zhang S., Imran A., Imran M.A. Mobile Edge Computing-Based Data-Driven Deep Learning Framework for Anomaly Detection. IEEE Access. 2019; 7: 137656–137667. doi: 10.1109/ACCESS.2019.2942485.

[17] Qin X., Tang S., Chen X., Miao D., Wei G. SQoE KQIs anomaly detection in cellular networks: Fast online detection framework with Hourglass clustering. China Commun. 2018; 15:25–37. doi: 10.1109/CC.2018.8485466.

[18] Hussain B., Du Q., Ren P. Semi-supervised learning based big data-driven anomaly detection in mobile wireless networks. China Commun. 2018; 15:41–57. doi: 10.1109/CC.2018.8357700.

[19] Akhi, A. B., Kanon, E. J., Kabir, A., &Banu, A. (2019).Network Intrusion Classification Employing Machine Learning: A Survey. (Doctoral dissertation)Department of Computer Science and Engineering, United International University, Bangladesh.

[20] Alizadeh, H., Khoshrou, A., &Zuquete, A. (2015). Traffic classification and verification using unsupervised learning of Gaussian Mixture Models. In2015 IEEE international workshop on measurements & networking (M&N). 1-6. IEEE.

[21] Amangele, P., Reed, M. J., Al-Naday, M., Thomos, N., & Nowak, M. (2019). Hierarchical Machine Learning for IoT Anomaly Detection in SDN. In2019 International Conference on Information Technologies (InfoTech). 1-4. IEEE.

[22] Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H., & He, Y. L. (2017). Fuzziness based semisupervised learning approach for intrusion detection system.Information Sciences, 378, 484-497.

[23] Aung, Y. Y., & Min, M. M (2018). An analysis of K-means algorithm based network intrusion detection system. Advances in Science, Technology and Engineering Systems Journal, 3(1), 496-501.

[24] Bauer, F. C., Muir, D. R., &Indiveri, G (2019). Real-Time Ultra-Low Power ECG Anomaly Detection Using an Event-Driven Neuromorphic Processor. IEEE Transactions on Biomedical Circuits and Systems, 13, 1575–82. 2019.2953001

[25] Bhati, B. S., Rai, C. S., Balamurugan, B., & Al-Turjman, F. (2020). An intrusion detection scheme based on the ensemble of discriminant classifiers.Computers & Electrical Engineering, 86, 106742.