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.v11i5.6692
***Article Received**: 05 March 2023 **Revised**: 22 April 2023 **Accepted**: 10 May 2023*

Anomaly Recognition in Wireless Ad-hoc Network by using Ant Colony Optimization and Deep Learning

Allen Paul L.Esteban
MSIT Faculty, Graduate School Department,
Nueva Ecija University of Science and Technology, Philippines.
estebanallenpaul@gmail.com

Abstract: As a result of lower initial investment, greater portability, and lower operational expenses, wireless networks are rapidly replacing their wired counterparts. The new technology that is on the rise is the Mobile Ad-Hoc Network (MANET), which operates without a fixed network infrastructure, can change its topology on the fly, and requires no centralised administration to manage its individual nodes. As a result, MANETs must focus on network efficiency and safety. It is crucial in MANET to pay attention to outliers that may affect QoS settings. Nonetheless, despite the numerous studies devoted to anomaly detection in MANET, security breaches and performance difficulties keep coming back. There is an increased need to provide strategies and approaches that help networks be more safe and robust due to the wide variety of security and performance challenges in MANET. This study presents outlier detection strategies for addressing security and performance challenges in MANET, with a special focus on network anomaly identification. The suggested work utilises a dynamic threshold and outlier detection to tackle the security and performance challenges in MANETs, taking into account metrics such as end-to-end delay, jitter, throughput, packet drop, and energy usage.

Keywords: MANET; QoS; Anomaly; EED;

I. Introduction:

Finding entities that significantly deviate, are incomparable, and are inconsistent with the majority of data in various domains is the goal of anomaly detection research, which is a key research subject [1]. The sudden boom of available data has shown a unique research trend. This opens up exciting new opportunities for anomaly detection research as well as new obstacles. Anomaly detection is useful in many fields, including the research and monitoring of data from the network traffic, web log, medical domain, financial transactions, transportation domain, and many more. In literature, the terms anomalies and outliers are often used interchangeably [2]. Anomaly and outlier are used interchangeably throughout this paper. The performance of Mobile Adhoc Networks is commonly measured using anomaly detection (MANET). Because to the difficulties inherent in the associated protocols, MANET has become a popular field of study in recent years. Users can connect to a dynamic network architecture wherever they are thanks to MANETs. Because of the availability of powerful and inexpensive tiny devices, MANETs can rapidly expand on their own. In order to facilitate communication and the sharing of services and data, these devices are equipped with the means to detect the presence of other devices and to perform the necessary organisation. Due to the distributed nature of MANETs, each node is responsible for its own message delivery and network upkeep. Because of the fluid nature of MANET topology, there are a number of challenges unique to message routing. When compared to wired networks, MANETs are more susceptible to malicious attacks due to their mobile nodes, dangers to compromised nodes in the network, limited security, changeable topology, scalability, and lack of centralised management [3]. Problems with QoS metrics including throughput, packet delivery, connection capacity, energy consumptions, end-to-end delay, etc. must be addressed in a MANET. In addition to the energy, route stability, and resource estimation needs of a MANET, there are other QoS requirements that need to be met. It is possible, and often recommended, to keep some supplies on hand at various points along the best path.

1.1. Value of Individual Variables in MANETs:

Self-reconfiguring and nomadic in nature, MANETs are wireless networks made up of autonomous nodes. The MANET network topology is constantly shifting in an unpredictable manner. The military, search-and-rescue operations, disaster management, home networks, mobile conferencing, etc. are just a few of the many applications of MANET technology. In a basic MANET, wireless nodes are clustered together without any kind of fixed infrastructure, and they exchange information via packet transmission.

Multiple ad hoc networks (MANETs) are vulnerable to intrusion because of their dynamic topology, transmission between nodes over wireless media, and lack of adequate administration and control of communications. As a result, there are a lot of tricky problems that need fixing in MANETs [4]. Some of the most pressing issues that MANET must address are the following: a lack of centralised control; insufficient resources; a dynamic topology; and a network that is both small in scope and large in scale. In addition, there are problems with the lack of a borderline, scalability, power constraints, and numerous performance challenges, such as bandwidth availability. Maintaining both high performance and safe inter-node communication is difficult.

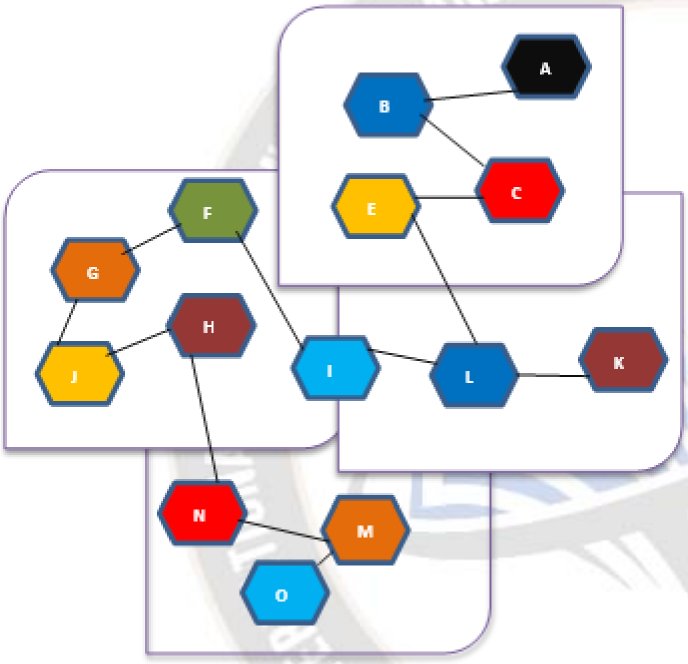

Figure I: Route Establishment Process in Wireless Netwrok.

In order to classify nodes as normal or abnormal, a communication structure is developed for MANET nodes. Outlier detection in the massive dataset generated in MANETs is the traditional method for identifying such structures. The accuracy of data analysis is enhanced by the identification of outliers, which in turn decreases the transmission overhead of erroneous data and enhances the overall results [5]. Furthermore, outlier identification is an effective technique for identifying items in wireless network data that do not conform to the norm. The network's safety is further confirmed by the fact that the discovered data objects indicate data values produced by hostile sensors, which may indicate attacks from adversaries.

1.2. Difficulties in Finding Anomalies in MANET

As was previously said, outliers are anomalous trends that stand in stark contrast to the average. This strategy may look easy, however completing it is incredibly difficult for the reasons below. It is difficult to define a normal region in an outlier detection method because there is often a thin boundary between what is considered normal and what is considered abnormal in any given application, making it difficult to compute all possible normal items or objects in a dataset. Objects at the limits have a higher chance of being misidentified as abnormal when they are actually within the expected range [6]. In addition, training data with labels is difficult to come by. Outlier detection is widely used in many fields, including MANETs. As a result of their fluid nature, MANETs are vulnerable to a variety of security risks, making it necessary to employ adaptive security measures. From this vantage point, anomaly-based intrusion detection systems aid in safeguarding networks from harmful intrusions. The following are some of the obstacles that must be overcome before outlier detection may be used in MANETs for intrusion detection to improve network safety and efficiency.

1. As there is no single, reliable supervisor node in MANETs, the responsibility for keeping attack signatures up-to-date falls on the networks themselves.
2. The robustness and highly dynamic topology of a network enhance the likelihood that the routing tables will need to be generated and adjusted repeatedly, requiring more resources and a larger number of packets to be transmitted than would otherwise be the case.
3. Since MANETs are open networks with no clearly defined boundaries, security is a primary problem. It is essential to deploy a cooperative detection system for the detection and prevention of major threats if security is to be properly implemented [7].

II. Existing Work Done:

It is useful in many contexts to be able to identify global outliers, which signal a departure from the norm. When a large number of packets are sent in a short amount of time, for instance, an intrusion detection system may take notice. When anomalies are uncovered by such systems, it is assumed that the communicating device has been hacked [8]. Distinguishing proof of global outliers can be achieved at varying network stages depending on the network design. The information needed to identify anomalies is sent to a single location, or sink node, in a decentralised architecture. Because of the extra time and effort required for communication, the mechanism delays responses. The "cluster head" in a clustering-based design collects information from nodes within its sphere of influence and then identifies anomalies. The response time and energy efficiency are both enhanced by this approach. It's worth noting that isolated nodes with a copy of the global estimator model obtained from the sink node can spot worldwide anomalies [9]. For sensor network data gathering purposes, the authors offer a histogram-based technique for identifying global outliers. As opposed to collecting raw data for centralised processing, this method collects histogram information in an effort to lessen communication costs. Histogram information is used by the sink to isolate the data distribution from the network and remove the typical data points. By retrieving additional histogram data from the system, outliers can be identified. Distinguishing proof of outliers is attained by either exceeding a predetermined threshold distance or by ranking among all outliers [10]. The technique only considers one-dimensional data, and remembering more histogram data from the entire network will generate unnecessary communication overhead. Those who are geographically isolated typically think about those who live nearby. Using a point's calculated distance from all the other locations in the dataset, distance-based methods actively seek find anomalies. Both "global" and "local" outliers can be discovered [11]. Data points that are outliers for their k nearest neighbours are considered "local" outliers, in contrast to the "global" outliers that are identified by a larger distance threshold. Each data point in a constant environment was given an outlier score based on the Local Outlier Factor (LOF), which is discussed and defined in. The LOF method is widely used, and numerous variants on this methodology have been devised, because it achieves respectable detection performance in nonhomogeneous densities without accounting for the distribution of the data set. Local outlier recognition techniques reduce communication overhead and boost scalability by distinguishing local outliers at individual sensor nodes [12]. The MANET provides two options for determining nearby outliers. Then, each node can tell an abnormal value by looking back at its own past data. The alternative is for each sensor node to collect readings from its neighbours in order to collectively recognise the abnormal levels, rather than relying solely on the interpretations it has independently made in the past. In contrast to the prior method, the next method improves the accuracy and robustness of outlier detection by capitalising on spatiotemporal correlations among sensor data [13].

A contextual outlier is a data point whose value significantly deviates from the rest of the objects in the same context. In a different setting, an outlier would not be considered exceptional. Due to their connection to a particular context that is outlined as part of the problem, contextual outliers are also known as conditional outliers [14]. Significant outliers of this kind can be found in time series data, which is collected over a specific time frame. In contrast to global outliers, which are only related to behavioural attributes, contextual outliers are also related to contextual attributes. If a group of observations deviates significantly from the rest of the dataset as a whole, we call them an outlier group [15].

Several independent Intrusion Detection System (IDS) agents operating at the local level identify potential attacks. On the other hand, researchers gather data locally, combine it, and then use it to offline acclimatise the classifier models. In the testing phase, the local IDS agent uses the resulting classification rule to conduct detection on its own. Combining the association rules algorithm with the frequent episodes algorithm, a new agent-based intrusion detection system architecture has been presented [16-18]. To characterise programme behaviour, different algorithms are used to compute intra-audit and inter-audit record patterns. In order to protect Internet-connected users from DoS assaults utilising signature and anomaly-based methods, a hybrid IDS with SVM classifier has been developed. The IDS produces very precise results. As an extension of Mobile Ad hoc Networks (MANETs), Opportunistic Networks (OppNets) allow for message flow between nodes in the network without requiring an already established path between them [20-22]. This raises doubts about the node's potential as a future carrier node, which could slow down the transmission of messages. Researchers have suggested a protocol called K-Nearest Neighbour based Routing (KNNR) that uses the K-Nearest Neighbour (KNN) method to store the past actions of nodes in a dataset and then look for occurrences that are similar to intermediate node based on network factors [23-24].

III. Prime Objective of this Research:

Below, we detail the study's intended outcomes for researchers.

i) Investigate anomaly scoring as a means of identifying outliers in the context of network defence against denial-of-service attacks.

ii). The second objective is to evaluate the suggested outlier detection mechanism in MANET routing protocols in terms of throughput, end-to-end delay jitter, and energy consumption in networks.

Iii). To protect MANET's cryptographic properties and accessibility through anomaly detection.

IV. The Proposed Work:

The usage of mobile sensor devices is suggested in this paper as a means of identifying and avoiding the occurrence of previously unrecorded data caused by constraints placed on available resources. The combined strategy that has been developed is superior to the methods that are now considered state-of-the-art in numerous essential areas, such as forward and backward secrecy, compression, and collision resistance. In addition, a hybrid technique can be produced by merging a number of different standard key management protocols. It has been determined that the proposed method for the identification and prevention of outliers performs better than existing systems that are equal in terms of energy efficiency, scalability, and the optimization of readily available resources. Comparisons are made between the different detection rates. It was discovered that the number of nodes has a detrimental effect on the Average Local Wrongly Calculated Anomaly Ratio (ALWCAR), which is the average value of the Wrongly Calculated Anomaly Ratio. [Citation needed] (WCAR).

A node is an outlier if its anomaly score falls below a predetermined threshold. Algorithms 1-3 are used to calculate this threshold value in order to single out an outlying node; algorithm 4 is used to choose a cluster's head and to single out an outlier using the threshold value.

To determine the upper bound on the anomaly score that can be used for outlier detection, Algorithm 1 determines the threshold value for a local event if the corresponding connection is IDLE. The network nodes' STD anomaly scores are compared to this value. The anomaly score differential at the present node may be below or over the set threshold value for the network. If the new node's anomaly score is lower than the network's threshold limit, it is used as the network's STD value. The current anomaly score is used as the network threshold if the difference between the current node and the previous node is greater than the threshold value.

Algorithm 1 is as follows:

```
If CA-LA< STD        [CA: Current Anomaly; LA: Last anomaly; STD: Standard Deviation]
CT=STD (CA)            [CT: Current Threshold]
LA=CA
```

If a link is busy, the threshold for a local event is determined by Algorithm 2. For optimal efficiency, it's preferable to have many favourable outcomes and few unfavourable ones. The algorithm 2 is as follows:

```
If (positive parameter > QoS positive threshold) and delay, (Energy consumed < QoS
negative threshold)
If (CA-LA)< STD
CT= STD (CA)
LA=CA
Else
NO alteration in LA
```

If packet loss is significant, Algorithm 3 determines a local event's critical threshold. In the presence of severe packet loss or severe packet drop, the score for the anomaly fluctuates dramatically. A network's threshold packet loss or packet drop value is the mean value of packet loss or drop across the whole network. The algorithm 3 is as follows:

```
If (PL< QoS –ve threshold)
Till (PL<QoS –ve threshold)
T=0
If T==0
LA=CA
Else
LA= 2xLA
Else
No alteration in LA
```

The situation where the outliers are found and the cluster leaders are chosen is described in Algorithm 4. The cluster's leader is the node with the most energy, and anomalous nodes are identified by comparing their energies to a threshold value. This information is relayed to the cluster head and other nodes so that they can avoid having to communicate with the affected node directly. This saves power for intermediate and final nodes, maximising efficiency.

1. Cluster head should be set to the node with the highest energy
2. Establish limits (value)
3. If node (iroute)'s reply is greater than the defined threshold, then (value)
4. As soon as the node is identified as an outlier, an alarm is sent to the cluster's leader and all other nodes in the cluster.
5. Avoid routing through the node if it is an outlier
6. Discharge energy calculation

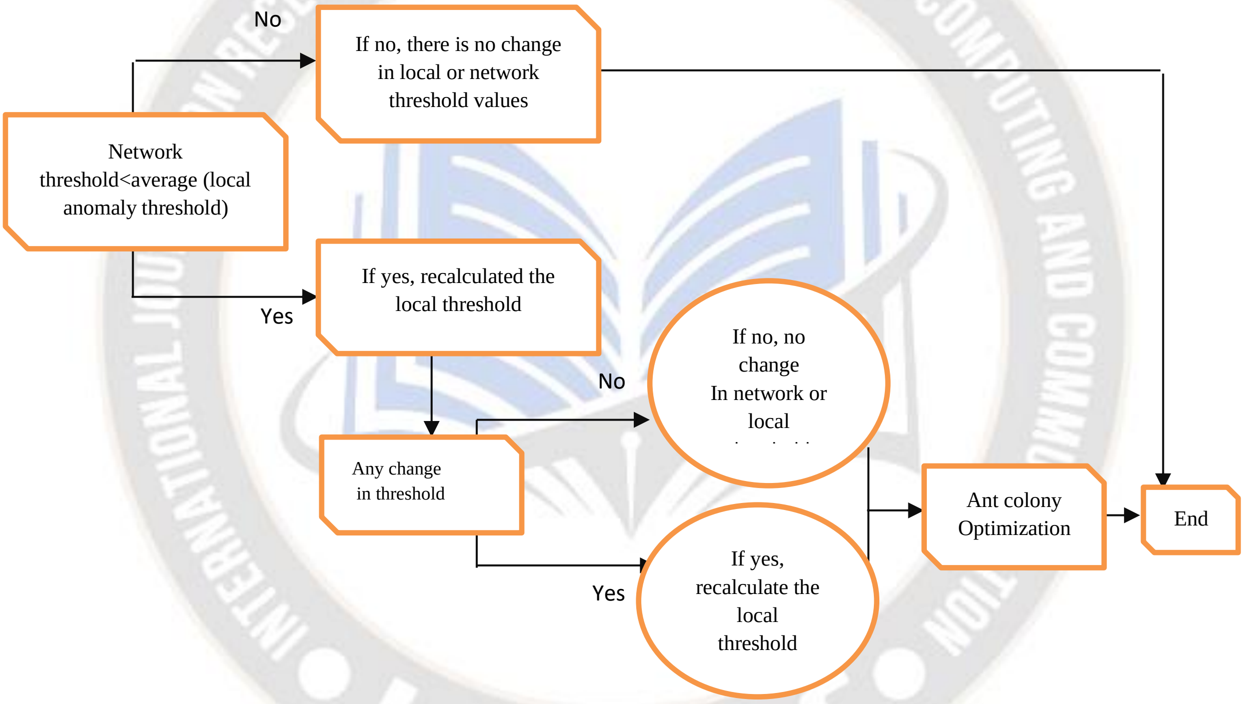
No
If no, there is no change in local or network threshold values
Network threshold<average (local anomaly threshold)
If yes, recalculated the local threshold
Yes
No
If no, no change In network or local
Any change in threshold
Ant colony Optimization
End
Yes
If yes, recalculate the local threshold

Figure 1: The Proposed Work Flow Diagram.

Adaptive combinatorial optimization (ACO) is a meta-heuristic strategy for dealing with intractable combinatorial optimization problems. Inspired by the behaviour of real-world ants, ACO methods cast computational agents in the role of ants that lay down pheromone trails to communicate with one another and find the most direct path from the nest to the source of food. The following generations of ants will follow these pheromone trails to get the best possible answer. Ants employ an energy-efficient strategy and an incredible capacity to regulate the amount of food coming into the nest on both a communal and an individual basis to triumph over their harsh natural surroundings. At its final destination, the ant turns around and returns by its original route. Pheromone evaporation factor reduces pheromone concentration along all suboptimal routes. These swarm intelligence methods are put to use in areas as diverse as the management of unmanned vehicles, the mapping of planets, and the resolution of optimization problems involving multiple variables.

V. Result and Analysis:

In this study, we compare the performance of the proposed outlier detection mechanism across multiple MANET routing protocols and QoS factors in a network of 200, 500, and 1000

***Article Received**: 05 March 2023 **Revised**: 22 April 2023 **Accepted**: 10 May 2023*

nodes. Comparative examination of jitter for networks with 200-1000 nodes using the proposed outlier detection mechanism reveals that Zone Routing Protocol (ZRP) yields the lowest jitter value. Because it is a hybrid, ZRP is able to respond well to fluctuating network load. It is also observed that the jitter value rises as the network size grows larger. The reason for this is that an increase in network traffic also causes an increase in network overhead.

5.1 Energy Reduction: The term "energy reduction" is used to describe the total amount of power that is utilised by a network throughout the process of sending and receiving information. This value is extremely important for the routing process; but, once clusters begin to form, it also becomes an energy drain. Network Lifetime: This subsection assesses the network's expected lifespan in relation to the total network area. Network lifetime is the period that elapses before the first node dies from lack of power. The implemented scheme's energy efficacy can be gauged by its ability to assess the network's lifetime.

5.2. End-to-end delay: Reducing Reduced power consumption and increased reliability are two benefits of end-to-end (E2E) delay. Hence, less time spent waiting improves both efficacy and dependability. E2E delay measures how long it takes for a packet to go from one node to another. Time spent on tasks such as data processing, transmission, and reception are all factored into the end-to-end delay.

$$End\ to\ end\ Delay = Time\ for\ (Data\ transmission + Data\ processing + Data\ delivery\ ) \qquad (3)$$

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

$$Throughput = \frac{Forwaded\ data}{Transmission\ time} \qquad (4)$$

All the parameters are compared for different routing protocol and summarized below at Table I.

Table I: Evaluation parameters Comparison of Different Routing Protocol.

Routing Protocol	Jitter			End to End Delay			Throughput		
	200	500	1000	200	500	1000	200	500	1000
DSR	3	5	7	17	20	25	11	13	15
ZRP	1.15	1.34	1.78	10	15	20	12	18	24
OLSR	1.25	1.89	2.14	14	17	23	11	15	18

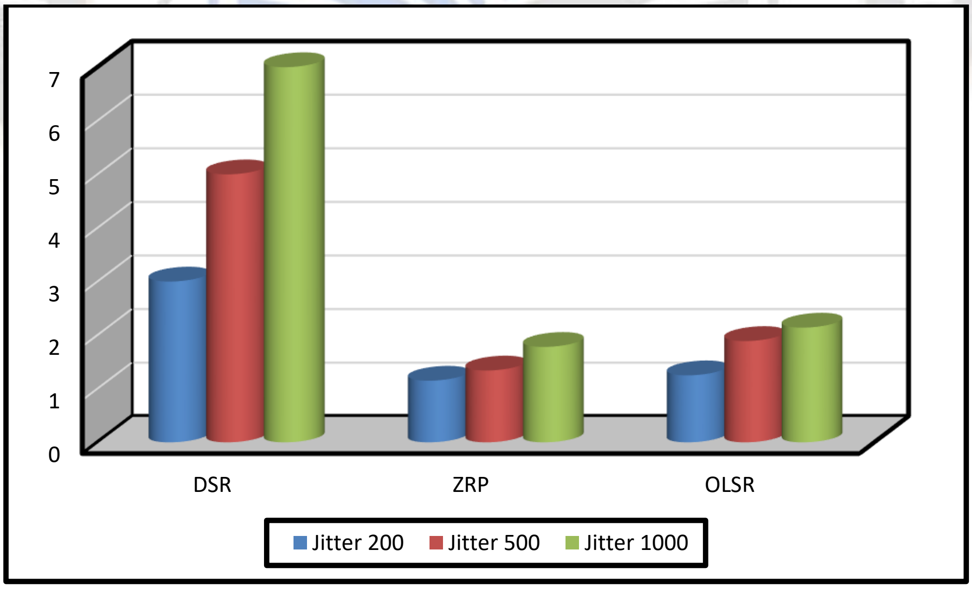

Figure II: Jitter Performance for different Routing Protocol.

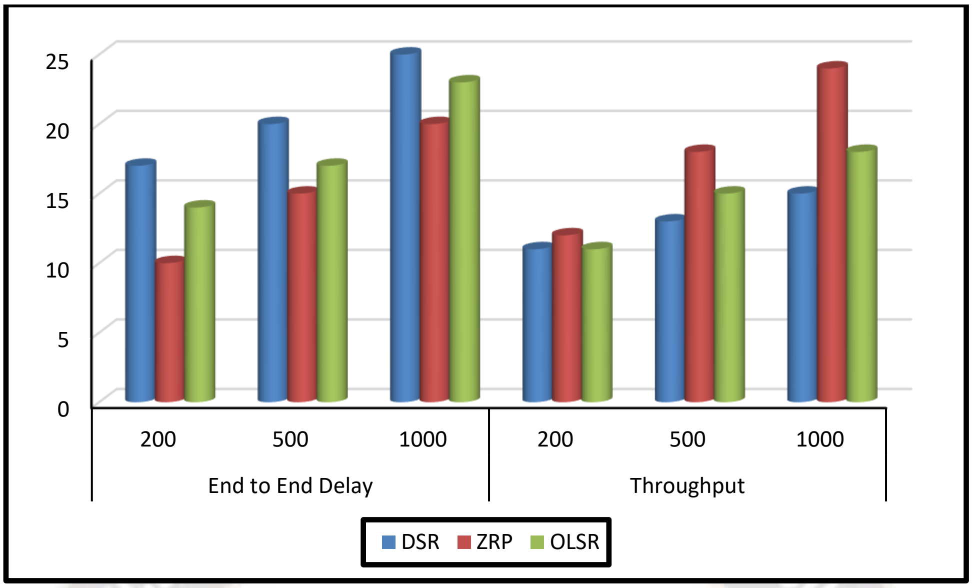

Figure III: Performance Comparison for Different Routing Protocol.

Figure III displays the results of a comparison of the end-to-end delay for networks with 200, 500, and 1000 nodes utilising the suggested outlier detection mechanism over three distinct MANET routing protocols (DSR, ZRP, and OLSR). ZRP is demonstrated to have the shortest end-to-end lag. When comparing end-to-end delays for networks with 200-1000 nodes, the DSR protocol has the longest latency thanks to the suggested outlier identification mechanism. Delay from beginning to finish grows as more nodes are added to the network. This is due to the fact that an increase in the network's size also results in an increase in the time it takes to complete tasks like processing and propagating messages. There is a significant delay in processing and dissemination because nodes are spending so much time processing a high number of requests.

Figure III displays the results of a comparison between the throughput of a network with 200-1000 nodes using the suggested outlier detection technique and the throughput of a network employing three of the five MANET routing protocols (DSR, ZRP, and OLSR). From a throughput standpoint, ZRP is seen to perform better than the other protocols. The reason for this is that ZRP prevents anonymous communication by segmenting the network into zones that can respond to changing conditions. As more nodes are added, more pathways can be established to the final destination, leading to a higher throughput. The likelihood of data successfully reaching its destination is improved when numerous pathways are established.

Table II: Energy Ingestion Comparison of Different Routing Protocol.

Routing Protocol	sender energy ingestion (mJ)			receiver energy ingestion (mJ)		
	200	500	1000	200	500	1000
DSR	2	5	7	1.2	2.5	4.1
ZRP	1.7	1.9	2.4	0.8	1.3	1.8
OLSR	2	4	5	1.1	2.6	4.2

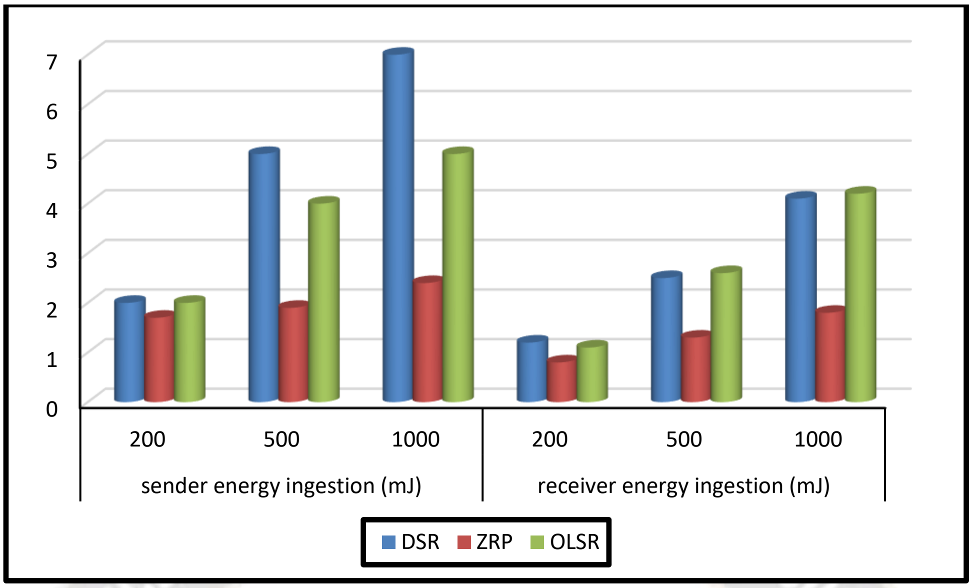

Figure IV: Energy Ingestion Comparison for Different Routing Protocol.

Figure IV displays the results of a comparison analysis of the average energy consumption of the sender for networks ranging in size from 200 to 1000 nodes, utilising the proposed outlier identification mechanism. In this study, we find that ZRP has the lowest average sender energy use, whereas the DSR protocol has the highest. Because the ZRP protocol builds a hierarchical network with interconnected nodes, messages can be sent and received quickly.

Once again, it is observed that ZRP's well-organized network results in the lowest average receiver energy use. When an unstructured network is used in DSR and OLSR protocols, there is a higher receiver energy consumption due to the numerous transmissions of the same packet and the increased likelihood of lost acknowledgment packets.

VI. Conclusion:

In this study, the suggested outlier detection technique using MANET routing protocols was used to conduct a comparative analysis of a number of various quality-of-service (QoS) metrics, such as jitter, end-to-end delay, throughput, and sender and receiver energy consumptions. Dynamic Source Routing (DSR), Zone Routing Protocol (ZRP), and Optimized Link State Routing Protocol are the MANET routing protocols studied here (OLSR). Comparative examination of jitter for networks with 200-1000 nodes using the proposed outlier detection mechanism reveals that Zone Routing Protocol (ZRP) yields the lowest jitter value. In addition, it is discovered that the jitter value grows as the network size grows in terms of the number of nodes. The reason for this is that an increase in network traffic also causes an increase in network overhead. The suggested outlier detection mechanism is used to compare the end-to-end delay of five different MANET routing protocols, revealing that ZRP has the lowest end-to-end delay and DSR the most. Delay from beginning to finish grows as more nodes are added to the network. This is due to the fact that an increase in the network's size also results in an increase in the time it takes to complete tasks like processing and propagating messages. By a wide margin, ZRP has the highest throughput compared to the other protocols. The reason for this is that ZRP prevents anonymous communication by segmenting the network into zones that can respond to changing conditions. As more nodes are added, more pathways can be established to the final destination, leading to a higher throughput. The likelihood of data successfully reaching its destination is improved when numerous pathways are established. The average sender energy usage is lowest for the ZRP protocol and highest for the DSR protocol, according to a comparison of the two. Timely message transmission is made possible via the ZRP protocol, which builds an organised, interconnected, semi-hierarchical network. Unstructured networks are used in DSR and OLSR protocols. Again, a comparison reveals that ZRP's organised network results in the lowest average receiver energy use.

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.

References:

[1] V. Justin, N. Marathe, and N. Dongre, “Hybrid IDS using SVM classifier for detecting DoS attack in MANET

application," in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017.

[2] M. Reza and S. Abyaneh, "Security analysis of Lightweight Schemes for RFID Systems," 2012.

[3] S. Parthasarathy, "Extraction of Outliers from Imbalanced Sets," pp. 2167–2172, 2016.

[4] K. D. Sharma, Aayush, S. Abhishek, and J. Kumar, "KNNR: K-nearest neighbour classification based routing protocol for opportunistic networks," in 2017 Tenth International Conference on Contemporary Computing (IC3), 2017.

[5] O. Yim, "Hierarchical Cluster Analysis: Comparison of Three Linkage Measures and Application to Psychological Data," Quant. methods Psychol., pp. 8–21, 2015.

[6] M. J. Embrechts, C. J. Gatti, J. Linton, and B. Roysam, Hierarchical Clustering for Large Data Sets. 2013.

[7] J. Hussain and S. Lalmuanawma, "Fusion of Misuse Detection with Anomaly Detection Technique for Novel Hybrid Network Intrusion Detection System," in Recent Developments in Intelligent Computing, Communication and Devices, 2017, pp. 73–87.

[8] G. Pu, L. Wang, J. Shen, and F. Dong, "A Hybrid Unsupervised Clustering-Based Anomaly Detection Method," Tsinghua Sci. Technol., vol. 26, no. 2, pp. 146–153, 2020.

[9] V. Rishiwal, S. Verma, and S. K. Bajpai, "QoS Based Power Aware Routing in MANETs," Int. J. Comput. Theory Eng., vol. 1, no. 1, pp. 49–54, 2013.

[10] V. Rishiwal, S. K. Agarwal, and M. Yadav, "Performance of AODV protocol for H-MANETs," Proc. - 2016 Int. Conf. Adv. Comput. Commun. Autom. ICACCA 2016, pp. 1–4, 2016.

[11] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of Service Defence for Resource Availability in Wireless Sensor Networks," IEEE Access, vol. 6, pp.6975–7004, 2018.

[12] J. Karlsson, G. Pulkkis, and L. S. Dooley, "A packet traversal time per hop based adaptive wormhole detection algorithm for MANETs," 2016 24th Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2016, 2016.

[13] S. Yadav, M. C. Trivedi, V. K. Singh, and M. L. Kolhe, "Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme," 2017 4th IEEE Uttar Pradesh Sect. Int. Conf. Electr. Comput. Electron. UPCON 2017, vol. 2018–Janua, pp. 1–4, 2018.

[14] A. Kumar, K. Gopal, and A. Aggarwal, "Design and analysis of lightweight trust mechanism for secret data using lightweight cryptographic primitives in MANETs," Int. J. Netw. Secur., vol. 18, no. 1, pp. 1–18, 2016.

[15] A. Kumar, K. Gopal, and A. Aggarwal, "Novel trusted hierarchy construction for RFID sensor-based MANETs using ECCs," ETRI J., vol. 37, no. 1, pp. 186–196, 2015.

[16] S. Henningsen, S. Dietzel, and B. Scheuermann, "Challenges of misbehaviour detection in industrial wireless networks," Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST, vol. 223 LNICST, pp. 37–46, 2018.

[17] M. Wazid and A. K. Das, "An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks," Wirel. Pers. Commun., vol. 90, no. 4, pp. 1971–2000, 2016.

[18] Xuxiang, W.L.Q.H.B. Multidimensional Data Anomaly Detection Method Based on Fuzzy Isolated Forest Algorithm. Comput. Digit. Eng. 2020, 48, 862–866.

[19] Zhou, J.C. Satellite Anomaly Detection Based on Unsupervised Algorithm. Master's Thesis, Wuhan University, Wuhan, China, May 2020.

[20] Hariri, S.; Kind, M.C.; Brunner, R.J. Extended Isolation Forest. IEEE Trans. Knowl. Data Eng. 2021, 33, 1479–1489.

[21] Wang, Z.; Zhou, Y.; Li, G. Anomaly Detection by Using Streaming K-Means and Batch K-Means. In Proceedings of the 2020 5th IEEE International Conference on Big Data Analytics (ICBDA), Xiamen, China, 8–11 May 2020; pp. 11–17.

[22] Ying, S.; Wang, B.; Wang, L.; Li, Q.; Zhao, Y.; Shang, J.; Huang, H.; Cheng, G.; Yang, Z.; Geng, J. An Improved KNN-Based Efficient Log Anomaly Detection Method with Automatically Labeled Samples. ACM Trans. Knowl. Discov. Data 2021, 15, 34.

[23] Wang, B.; Ying, S.; Cheng, G.; Wang, R.; Yang, Z.; Dong, B. Log-based anomaly detection with the improved K-nearest neighbor. Int. J. Softw. Eng. Knowl. Eng. 2020, 30, 239–262.

[24] Xu, S.; Liu, H.; Duan, L.; Wu, W. An Improved LOF Outlier Detection Algorithm. In Proceedings of the 2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Dalian, China, 28–30 June 2021; pp. 113–117.