International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

# Ranking Based Security Scheme with Attack Detection and Improved Network Security

**Rajesh B. Walde[1], Om Prakash[2], Dr. M. Sunil Kumar[3], Bipin Sule[4], Khan Vajid Nabilal[5], Dr. Usha C. Pawar[6]**

**Submitted:** 01/11/2022 **Revised:** 09/01/2023 **Accepted:** 01/02/2023

**Abstract:** In the diverse environment anomaly detection significant challenge for the efficient analysis of the data traffic monitoring, medical domain, transaction of financial data, web log, domain for transportation, wireless mobile network and so on. Wireless network comprises of the different factors such as ease of use and reduced running cost in the network. MANET network comprises of the infrastructure less, auto configured, dynamic topology and central administration in the network node. This paper concentrated on the examination of the challenges in the MANET attack security challenges and proposed an anomaly detection scheme. The proposed anomaly detection scheme incorporates the scoring procedure for the anomaly detection in the network. The anomaly detection score computes the ranking values in the MANET network for the analysis. The developed ranking-based anomaly detection scheme is defined as the Ranking Anomaly Score (RAS). The performance of the RAS model is evaluated in terms of throughput, Packet delivery rate (PDR) and end -to-end delay. The performance of the proposed RAS model is comparatively examined with the existing Hashing, AODV and RSA. The comparative analysis expressed that proposed RAS model achieves the maximum throughput of 1600 bits/sec, maxima PDR is 98% and end-to-end delay is measured as 14ms. Through analysis it is observed that proposed RAS model achieves improved performance compared with the conventional technique.

***Keywords:*** *MANET, Anomaly Score, Ranking, Attacks, network security.*

## 1. Introduction

Anomaly detection is a significant research issue that targets to find entities that are substantially divergent, incomparable, and inconsistent with the majority of data in diverse domains [1]. In recent years, a remarkable research concern is witnessed scintillated by the explosion of collected data. This presents novel prospects as well as challenges for research efforts in anomaly detection. Anomaly detection is beneficial in various arenas as investigation and monitoring of data related to network traffic, web log, medical domain, financial transactions, transportation domain, and many more. Anomalies and outliers are frequently used interchangeably in literature [2]. The word outlier and anomaly are interchangeably used in this work also. Anomaly detection is significantly used to evaluate the performance of Mobile Adhoc Network (MANET). MANET is a prevailing research area in recent years due to the challenges in the related protocols. MANETs enable users to connect with a dynamic infrastructure irrespective of topographical location. MANETs are selforganizing and grow at a rapid pace because of small, powerful, and cheap devices. These devices are capable of detecting the existence of the other devices and implement the required organization to enable communication and sharing of services and data [3]. MANETs are decentralized where nodes are accountable for the delivery of messages and network organization. Due to the dynamic topology of MANET, message routing involves various issues. MANETs are more vulnerable to malicious attacks when compared to wired networks because of mobile nodes, threats from compromised nodes in the network, restricted security, dynamic topology, scalability, and lack of centralized management. It is necessary to take care of anomalies in MANET that affect

[1] *Assistant Professor, G B Pant DSEU Okhla Campus III, New Delhi, India.*
*rajesh.walde@gmail.com*
[2] *Assistant Professor, Department of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India.*
*om.prakash@galgotiasuniversity.edu.in,*
*0000-0001-7599-9873*
[3] *Professor and programme Head, Department of CSE, School of computing, Mohan Babu University, Tirupati, Andhra Pradesh, India.*
*sunilmalchi1@gmail.com*
*0000-0002-1439*
[4] *Professor, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, India.*
*bipin.sule@vit.edu*
*0000-0003-1409-2156*
[5] *Associate Professor, Computer Engineering, KJ College of Engineering and Management Research, Maharashtra, India.*
*kvajid12@gmail.com*
*0000-0002-0999-9776*
[6] *Assistant Professor, Mechanical Engineering, Datta Meghe College of Engineering, Airoli, Navi Mumbai, Maharashtra, India.*
*usha.pawar@dmce.ac.in*
*0000-0002-6516-5354*

the QoS parameters throughput, packet delivery, link capacity, energy consumptions, and end-to-end delay, etc [4]. The QoS requirements that MANETs 2 should address include bit rate error, route length, delay, bandwidth, etc. in addition to explicit requirements of MANET viz. Energy, route stability and estimation of resources, etc. An optimum route is chosen and resources are held in reserve along the route, if feasible [5].

Due to their dynamic nature, MANETs are susceptible to several security threats and the development of adaptive security approaches becomes a challenge for such scenarios. In this perspective, anomaly-based intrusion detection mechanisms are helpful to protect the networks against malicious attacks [6]. To employ outlier detection in MANETs for intrusion detection to enhance security and performance few challenges have to be dealt with, which are listed below [7]. 1. There is no central or stable supervisory node hence attack signatures are to be maintained by a distributed method for enabling secure communication in MANETs. 2. Robustness and highly dynamic network topology intensify the probability that the routing tables are to be constructed and altered repeatedly, therefore it involves additional energy and a larger number of packets are to be transmitted which results in increased overhead. 3. Security is a major concern as MANETs are the open network, i.e. there is no demarcated boundary. To incorporate security a cooperative detection mechanism has to be employed for the detection and prevention of critical attacks. 4. New detection mechanisms have to be developed to deal with new and diverse attacks that require the design and implementation of protocols broadly classified as proactive, reactive, and hybrid. More sophisticated protocols and lighter mechanisms are to be designed for resource constraint networks that can provide optimal output. 5. The mobile sensor devices comprising MANETs have low computing capability and possess restricted memory so the network provides limited bandwidth [8]. An anomaly detection system for MANETs requires the interchange of compacted traffic among nodes which needs high bandwidth. 7 6. MANET nodes have limited battery capacity and power which requires consistent or periodic recharge which requires, either centralized or decentralized, a mechanism for attaining optimum quality-of-service. 7. The distributed environment of resource constraint MANET gives a threat to Intrusion Detection System (IDS). A completely secured MANET needs to have five features i) availability, (ii) confidentiality, (iii) authentication & authorization, (iv) key management, and (v) non-repudiation which are to be incorporated using lightweight mechanisms with limited hardware and software requiring lesser energy intake [9]. 8. The IDS in MANETs, when designed as a lightweight mechanism, can have errors when organizing data in the training phase and when the attack patterns change frequently.

## 2. Related Works

The intrusion detection system comprises various local IDS agents that detect probable local intrusions. Conversely, researchers accumulate data locally, unify it and later utilize it to acclimatize the classifier models offline. The local IDS agent thereafter carries out detection autonomously in the testing phase using the resultant classification rule. Another agent-based architecture for intrusion detection systems has been proposed in [10] based on the association rules algorithm and the frequent episodes algorithm. Various algorithms are employed for the computation of intra-audit & inter-audit record patterns for the description of program behavior. A hybrid IDS with SVM classifier has been proposed in [11] to attain outcomes with less training time to prevent Denial of Service (DoS) attacks for the users connected to the Internet using signature and anomaly-based methods for detection performance. The IDS yield results with high accuracy. Opportunistic Networks (OppNets) are the additions of Mobile Adhoc Networks (MANETs) that do not assume that there is a preexistent path between the source and the destination node and the transfer of message takes place through the intermediary nodes. This gives rise to a concern about the decision making related to adjacent nodes whether it will be an efficient carrier node in the future for the transfer of messages [12]. As a solution to the problem, Sharma et al. have proposed a protocol K-Nearest Neighbor based Routing protocol (KNNR) that records the former behavior of nodes in a dataset and looks for occurrences that are similar to intermediate node grounded on network parameters using K-Nearest Neighbor (KNN) algorithm. The results of the proposed algorithm are compared with Epidemic, HBPR, and ProPHET and the observations reveal that the KNNR protocol ably decreases overhead ratio, average latency, and average hop count 20 and increases the message delivery probability. In the same line, another algorithm has been proposed in [13], named energy-efficient genetic algorithm, based on the bounded end-to-end delay which is NP-complete.

In unsupervised methods, mostly data with normal features are grouped in diverse groups and outliers may be present far away from the groups with normal objects. However, in some cases, data do not follow a particular pattern. In the second scenario, there may be more false-positive rates, i.e. normal data can be identified as an outlier. There is a third scenario where some objects lie in a cluster that is far away from other clusters and these objects can be identified as clustered outliers. Unsupervised approaches are more suitable for wireless networks as compared to supervised and semi-supervised approaches [14]. There are the number of unsupervised clustering methods used by

different researchers for the detection of outliers. We can categorize unsupervised clustering based on their characteristics as partitioning-based, density-based, grid-based, model-based, and hierarchical-based clustering. Researchers have proposed different algorithms under each category.

CLARANS [15] is an improvement over the K-medoid scheme grounded on randomized search. It initiates with arbitrary choice of k nodes, and in particular succeeding stages, matches each node to a definite number of its neighbors for searching and attaining a local minimum. Once local minimum is achieved, CLARANS repeats this process for alternative minimum until an exact number of minima is achieved and it is unaffordable for clustering a large database. Moreover, clustering quality results are reliant on the sampling method and it is not constant and distinctive because of the features of randomized search. In [16] each point in a cluster comprises the least possible number of points in the neighbor of a given radius. It presents the concept of "density-reachable points" and based on which clustering is completed. The entire process of clustering ends when no new point is added to clusters. DBSCAN counts on the user's capability to choose suitable parameters of epsilon and minpts. DBSCAN is influential in determining clusters of arbitrary shapes. The limitations include: 1) chaining effect results in adverse conditions 2) The two essential factors epsilon and minpts are difficult to decide beforehand and need a critical method of parameter tuning.

## 3. Ranking Anomaly Score for the MANET Security

In the proposed RAS cluster zones in the network are kept into observation for identifying outliers in the network. Let us consider that during the time interval from $T_S$ to $T_E$, 'R' is the selected region for observation. Let window selected for the said stretch is $T_{WIN} = [T_s, T_E]$.The total number of windows selected for observation during the ith day is given by $T_{win}^{i-day} \in \{(T_S^1, T_S^1)\ (T_S^2, T_E^2)(T_S^3, T_E^3), \ldots\ldots, (T_S^n, T_E^n)\ \}$Similarly, the total number of windows selected for observation during the kth month is given by $T_{win}^{k-month}$and the total number of windows selected for observation during the lth year is given by and $T_{win}^{l-year}$.A node can be either in the active or passive state. The active state is represented as$MN_{active}$. An active state node acts as source, destination, intermediate and switching-on node while a passive node acts as sleep or switching-off node. An ideal node is neither considered an active nor a passive node. From the active or passive states of a node, the anomaly score is calculated. Anomaly score is calculated using the equation (1)

$$Anomaly\ Score = \left(MN_{Active}^{Attendee} - \left(AVG_{MNActive+MN\ sleep}^{Attendee}\right)\right)/STDEV \quad (1)$$

Where standard deviation (STDEV) calculated as in equation (2) - (4):

$$Avg = \sum_{k=0}^{n} \frac{s.RR_k}{n} \quad (2)$$

$$V = \sum_{k=0}^{n} \frac{(RR_k - Avg)^2}{n} \quad (3)$$

$$STDEV = \sqrt{V} \quad (4)$$

Standard deviation (STDEV) is computed using the equation (4) for the nodes instances X1, X2, X3, X4 with the broadcastr range of 10, 10, 20, and 100 for the number of packets per seconds. The estimated average (Avg), variance (V) and STDEV. With the proposed RAS the outlier detection for the security is computed based on the threshold limits. The figure 1 provides the flow chart of the RAS model in the attack prevention for improved security is presented.

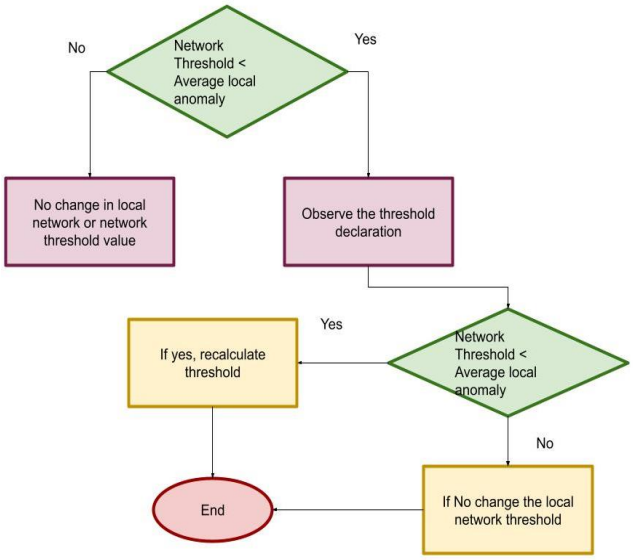


**Fig. 1:** Flow Chart for RAS

**Algorithm 1: Local event Threshold Limit in the IDLE**

1. if $\left(\left(Current_{anomaly} - Last\ _{anomaly}\right) < STDEV_{Network}\right.$
2. $Current_{Threshold} = STDEV_{Current\ Anomaly}$
3. $Last\ _{Anomaly} = Current_{Anomaly}$

Algorithm 2 calculates the threshold limit of the busy link in the local event. Various QoS parameters; throughput, bandwidth, packet delivery, link capacity, energy consumption, and end-to-end delay; are considered. Throughput, bandwidth, packet delivery, and link capacity are the QoS parameters that are considered for energy consumption and end-to-end delay with the negative

results. For high performance, positive results should be high and negative results should be lower.

Algorithm 2: Compute the local event threshold event for the BUSY link

Threshold Limit for a local event if a link is BUSY

1. If ((Throughput, Capacity of link, Bandwidth, PDR) >QoS_Positive_Threshold) AND ((End to End delay, Energy Consumption) <QoS_Negative_Threshold)
2. if $((Current_{anomaly} - Last_{anomaly}) \geq STDEV_{Network}$
3. $Current_{Threshold} = STDEV_{Current\ Anomaly}$
4. $Last_{Anomaly} = Current_{Anomaly}$
5. Else
6. No Change in $Last_{Anomaly}$

**Algorithm 1: Ranking Anomaly Score for the network security**

1. Compute active node list as A= [S, D, I] and passive node are computed as P= [U].
2. Classify the simulation time as the n-slots
3. iteration =1
4. list_Outlier =NULL
5. While $iteration \leq n$ do:
6. If iteration ==1 then
7. Estimate the number A and A+P nodes
8. Else-if iteration≥1 then
9. Compute overall number A fr the iteration slots for the average number A+P nodes
10. If ((Packet drop rate) >Anomaly Score_Negative_Threshold)
11. While ((Packet Loss) <Anomaly Score_Negative_Threshold)
12. Set t = 0
13. If (t == 0)
14. $Last_{Anomaly} = Current_{Anomaly}$
15. Else
16. $Last_{Anomaly} = 2 * Last_{Anomaly}$
17. Else
18. No Change in $Last_{Anomaly}$
19. Compute the node cluster = higher energy in the node
20. Compute the threshold value
21. If
22. Node route reply(i) > threshold (value)
23. Compute the anomaly score
24. For
25. Outlier_list in nodes
26. Discard communicated node
27. End for
28. Iteration=iteration+1
29. End-while

## 4. Results and Analysis

The number of the passive or active state of a node in the first and second slots are given. An anomaly score calculation for every node following 400 seconds is given. After and including the Second slot, total anomalies are calculated after regular intervals of 200 seconds. The plot of the anomaly score of 50 to 5000 nodes is given. Total number of outliers identified are 18, 28, 57, 97, 187, 247, 297 and 356 in 50, 100, 500, 1000, 2000, 3000, 4000 and 5000 nodes network respectively. Two processes by which inliers and outliers are detected in a network are conversed.For analyzing the proposed protocol simulation analysis of various nodes ranging from 50 to 5000 nodes is performed which are in the distributed manner over 1000 m x 1000 m area.

**Table 1:** Simulation Setting

| **Parameters** | **Values** |
|---|---|
| Numbers of nodes | 50 to 5000 |
| Network Interface | Wireless Phy |
| Radio Propagation Model | Ray Tracing |
| Interface Queue | Priority Queue |
| Channel type | Wireless Channel |
| MAC type | 802.11 |
| Mobility Model | Random Way Point Mobility |
| Max Packet in Queue | 50 |
| Data Rates | 5 Packet /second |
| Packet size | 512 bits |

| | |
|---|---|
| X dimension topology | 1000 mtrs |
| Y dimension topoogy | 1000mtrs |
| Antenna | Omni Antenna |
| Number of slots assigned to reader at stretch( ) | 1 |
| Simulation time | 2000 sec |
| Time of each slot | 10 msec |
| Velocity (Minimum to Maximum) | 0.3 m/s to 5 m/s |

A total of eight datasets have been considered for analysis purposes. The analysis is base don the consideration of the eight different datasets with the node traces. The cluster number ar computed as in anomaly score. In the table 2 the comparative analysis of the through for the proposed RAS is presented with the Hashing, AODV and RAS.

**Table 2:** Comparison of Throughput

| **Throughput (bits/sec)** | | | | |
|---|---|---|---|---|
| **No.of Nodes** | **Hashing** | **AODV** | **RSA** | **RAS** |
| 50 | 1100 | 1500 | 1800 | 2100 |
| 100 | 1700 | 2100 | 2300 | 4600 |
| 150 | 1900 | 2400 | 4500 | 5300 |
| 200 | 2100 | 2900 | 4900 | 6600 |
| 250 | 2400 | 3200 | 5200 | 7600 |
| 300 | 2600 | 3500 | 5700 | 8400 |
| 350 | 2900 | 3800 | 6300 | 9800 |
| 400 | 3200 | 4300 | 7800 | 11500 |
| 450 | 3500 | 4700 | 8300 | 13800 |
| 500 | 3700 | 5200 | 9200 | 16000 |

In tab;e 3 the PDR is estimated for the proposed RAS with the existing Hashing, AODV and RSA algorithm. The experimental analysis expressed that proposed RAS achieves the 99% PDR values.

**Table 3:** Comparative Analysis of PDR

| **PDR (%)** | | | | |
|---|---|---|---|---|
| **No.of Nodes** | **Hashing** | **AODV** | **RSA** | **RAS** |
| 50 | 73 | 76 | 86 | 91 |
| 100 | 70 | 78 | 84 | 94 |
| 150 | 74 | 81 | 89 | 96 |
| 200 | 71 | 84 | 83 | 93 |
| 250 | 68 | 80 | 81 | 90 |
| 300 | 69 | 79 | 83 | 98 |
| 350 | 67 | 77 | 87 | 96 |
| 400 | 70 | 74 | 89 | 97 |
| 450 | 72 | 76 | 86 | 99 |
| 500 | 74 | 73 | 84 | 95 |

With the developed model end-to-end delay is computed for the proposed RSA model with the existing hashing, AODV and RSA.

**Table 4:** Comaprison of End-to-End Delay

| **End-to -End Delay (ms)** | | | | |
|---|---|---|---|---|
| **No.of Nodes** | **Hashing** | **AODV** | **RSA** | **RAS** |
| 50 | 19 | 21 | 19 | 14 |
| 100 | 23 | 19 | 17 | 11 |
| 150 | 21 | 17 | 16 | 10 |
| 200 | 18 | 19 | 14 | 8 |
| 250 | 24 | 20 | 13 | 9 |
| 300 | 26 | 22 | 18 | 11 |
| 350 | 23 | 19 | 20 | 13 |
| 400 | 20 | 16 | 21 | 11 |
| 450 | 18 | 17 | 18 | 9 |
| 500 | 17 | 15 | 16 | 7 |

In the figure 2 – 4 the comparative analysis of the proposed RAS model is presented.

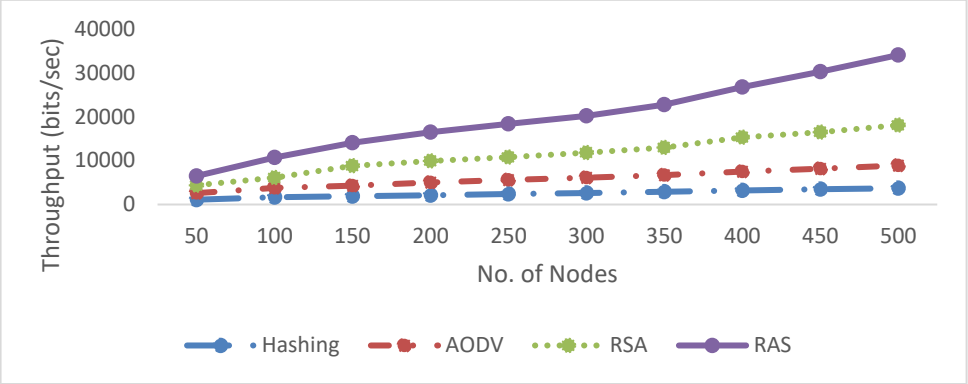


**Fig. 2:** Comparison of Throughput

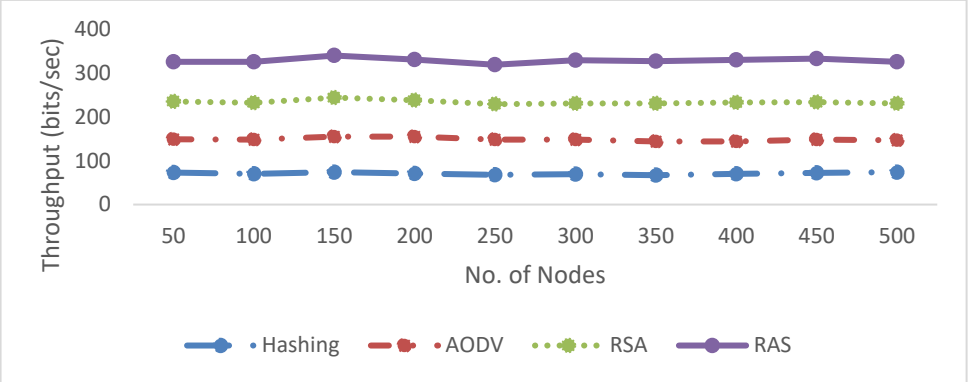


**Fig. 3:** Comparison of PDR

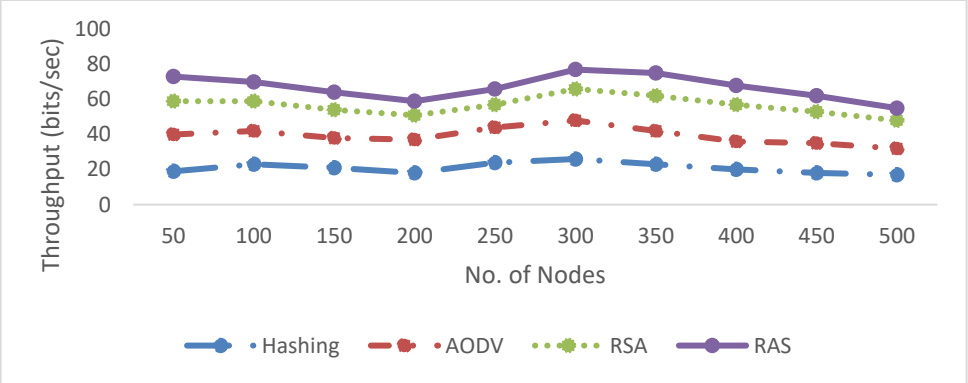


**Fig. 4:** Comparison of End-to-End delay

The proposed RAS achieves the maximal throughput of 16000 which is significantly higher than the hashing, AODV and RSA. In terms of the PDR estimation the RAS achieves the maximal value of 99% which is significantly minimal than the hashing, AODV and RSA. In terms of the end-to-ende delay estimation achieves the end-to-end delay value of 14 which is significantly less than the hashing, AODV and RSA model.

## 5. Conclusion

Network security is considered as the emerging constraints in the network for the estimated attacks in the MANET network. The security in the network is improved with the computation of the anomaly score in the network for the attack classification. The proposed model ranking based anomaly score is computed for the analysis of attack in the network. The performance of the proposed RAS is estimated as higher throughput and PDR rate compated with the hashing, AODV and RSA. The proposed RAS model achieves the ~5 % increase in the throughput and ~4% increases in the PDR and ~3% minimal than the end-to-ende delay in the network.

## References

[1] Jim, L. E., Islam, N., & Gregory, M. A. (2022). Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes. *Computers & Security*, *113*, 102538.

[2] Banerjee, B., &Neogy, S. (2021, December). A brief overview of security attacks and protocols in MANET.

In *2021 IEEE 18th India Council International Conference (INDICON)* (pp. 1-6). IEEE.

[3] Veeraiah, N., Khalaf, O. I., Prasad, C. V. P. R., Alotaibi, Y., Alsufyani, A., Alghamdi, S. A., &Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. *IEEE Access*, *9*, 120996-121005.

[4] Arappali, N., & Rajendran, G. B. (2021). MANET security routing protocols based on a machine learning technique (Raspberry PIs). *Journal of Ambient Intelligence and Humanized Computing*, *12*(6), 6317-6331.

[5] Kowsigan, M., Rajeshkumar, J., Baranidharan, B., Prasath, N., Nalini, S., & Venkatachalam, K. (2021). A novel intrusion detection system to alleviate the black hole attacks to improve the security and performance of the MANET. *Wireless Personal Communications*, 1-21.

[6] Rathish, C. R., Karpagavadivu, K., Sindhuja, P., &Kousalya, A. (2021). A Hybrid Efficient Distributed Clustering Algorithm Based Intrusion Detection System to Enhance Security in MANET. *Information Technology and Control*, *50*(1), 45-54.

[7] Tu, J., Tian, D., & Wang, Y. (2021). An active-routing authentication scheme in MANET. *IEEE Access*, *9*, 34276-34286.

[8] Simpson, S. V., & Nagarajan, G. (2022). Security challenges and attacks in MANET-IoT systems. In *Enterprise Digital Transformation* (pp. 159-201). Auerbach Publications.

[9] Sivapriya, N., & Mohandas, R. (2022). Analysis on Essential Challenges and Attacks on MANET Security Appraisal. *JOURNAL OF ALGEBRAIC STATISTICS*, *13*(3), 2578-2589.

[10] Shukla, M., Joshi, B. K., & Singh, U. (2021). Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. *Wireless Personal Communications*, *121*(1), 503-526.

[11] Ponnusamy, M. (2021). Detection of selfish nodes through reputation model in mobile adhoc network-MANET. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(9), 2404-2410.

[12] Das, M. V., Premchand, P., & Raju, L. R. (2021). Security Enhancing based on Node Authentication and Trusted Routing in Mobile Ad Hoc Network (MANET). *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(14), 5199-5211.

[13] Ramphull, D., Mungur, A., Armoogum, S., &Pudaruth, S. (2021, May). A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. In *2021 5th international conference on intelligent computing and control systems (ICICCS)* (pp. 204-211). IEEE.

[14] Vidhya Lakshmi, G., & Vaishnavi, P. (2022). An Efficient Security Framework for Trusted and Secure Routing in MANET: A Comprehensive Solution. *Wireless Personal Communications*, *124*(1), 333-348.

[15] Sharma, R. S., Keswani, B., & Goyal, D. (2022). Analysis of routing and security issues in OLSR protocol for video streaming over MANET. *Journal of Discrete Mathematical Sciences and Cryptography*, 1-9.

[16] Korir, F. C., & Cheruiyot, W. (2022). A survey on security challenges in the current MANET routing protocols. *Global Journal of Engineering and Technology Advances*, *12*(01), 078-091.