International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I9P232

Volume 70 Issue 9, 330-336, September 2022
© 2022 Seventh Sense Research Group®

Original Article

An Efficient and Secure Routing in MANET using Trust Model

Anugraha[1], Krishnaveni[2]

[1]*Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Tamilnadu, India*
[2]*Department of Computer Science and Engineering, Baselios Mathews II College of Engineering, sasthamcotta, kollam, Kerala, India*

[1]*Corresponding Author : ganu7665@gmail.com*

Received: 11 May 2022 Revised:12 July 2022 Accepted: 16 September 2022 Published: 30 September 2022

Abstract *- MANET is utilised in various applications due to its ability to the faster establishment of networks. The network will run well if mobile nodes trust one another and collaborate. Routing is difficult, and vulnerabilities are regularly exposed due to the frequent connection failures and dynamic topology induced by node mobility. As a consequence, security measures that can reduce the impacts of multiple assaults should be included in the MANET's routing. This research proposes a node trust evaluation approach based on cluster structure and a trust-based model security routing (TSR). The proposed technique used a hierarchical structure to improve the efficiency of node reliability evaluation. Because it assures node reliability evaluation, path establishment between nodes, and safe data exchange, the proposed method in this research can sustain network performance in the presence of hostile nodes. The integrity of data transfer is increased via node-to-node key exchange without CA. The suggested trust-based model security routing strategy outperformed the competition regarding packet delivery ratio, throughput, average delay, and packet loss.*

Keywords *- Adhoc, MANET, Trust, Routing, Performance.*

1. Introduction

Because of the increased use of simpler, more powerful wireless nodes and smaller networks in recent years, MANETs have received a lot of attention [1]. MANETs are self-organizing, multi-hop networks with a highly unpredictable and dynamic topology, in which any node can be a receiver, sender, or router. MANET offers peer-to-peer communication between nodes without depending on centralised resources or established infrastructure. Because mobile nodes rely on batteries for power, MANET has spent a lot of time researching energy-efficient routing solutions. MANETs are ideal for military surveillance, environmental monitoring, and disaster relief applications since they can be deployed fast and easily [2]. Because the mobile nodes operate as routers, it can allow multiple pathing to neighbour nodes and execute dynamic routing in route settings. Routing for QoS is a critical role in MANETs. [3]. Because nodes only interact with each other when they are within communication range, establishing an effective and safe routing system that can also preserve QoS is a challenging task for MANETs. Since the node-to-node link and channel vary dynamically, it is hard to verify QoS leads to frequent node failure and results in nodes connecting with other nodes [4]. A key challenge in MANETs is security because rogue nodes might purposefully misbehave, altering packet contents and disrupting packet routing to targeted destinations, decreasing packet delivery ratios and reliability. The terms "security" and "trust" are often used interchangeably. When it comes to trust-based security, the amount of access privilege for security protection rises in parallel with the level of trust. The proximity of relationships between entities that engage in a protocol exchange can be described as trust in MANETs. Social trust is based on social ties such as privacy, honesty, friendship, and closeness, while QoS trust is based on reliability [5]. Some suggestions for safeguarding the routing process in MANETs have previously been made [6]. Incorporating "trust" into the hostile environment can aid nodes in efficiently observing and anticipating nearby node behaviour. In a highly dynamic system where nodes must rely on one another to achieve their common goals, the concept of trust is extremely important [7]. In MANETs, trust-based routing is a viable solution for dealing with security issues posed by malevolent nodes by finding and segregating untrusted nodes [8].

2. Related works

The energy-aware on-demand routing protocol, introduced by Rajendra Prasad P and Shivashankar [9], is a unique and energy-efficient shortest route routing technique.

Depending on the routing condition, the protocol maximises the MANET's lifetime. MANET's energy-efficient routing constructs paths among the mobile nodes and protocol operations as long as the network's energy is available. The method is designed to reduce transmitter and receiver or idle power usage when a node in the network is in sleep mode. Quy et al. [10] designed a QoS-aware on-demand routing protocol for urban-MANET applications. This technique allows the method to function in adaptive and admission modes to make the suggested solution more viable. Sahu et al. [11] offered a new protocol for MANET utilising the recoil method, which saves energy while providing optimal performance. It outperforms all other AODV-based algorithms because the nodes use a changing recoil-off-time mechanism to intelligently transmit packets to their destination. The method minimises the number of communications and extends the network's lifetime.

Choi et al. [12] designed MANET-oriented local flooding using an on-demand routing system that decreases flooding overhead while providing effective alternate routes between nodes. Saha et al. [13] developed a unique trust-based that uses an idea that fluctuates based on how many packets are dropped. Direct and indirect methods are used to monitor fidelity. The system's main purpose is to design a technique that uses battery power and node trust when deciding which nodes to use for secure data transfer. Duvvuri et al. [14] take up the research task of inventing an effective fault-resistant routing system for MANET. A fault-tolerant routing system was created using an ANFIS. The numerical estimation-based fault-tolerant routing methods are discussed.

Hinge et al. [15] suggested a model that relies on network features. The opinion trust of intermediate nodes is computed in this solution, and a decision is made on using a certain transmission channel based on this value. Due to the limited radio range, communication in MANETs must be done through intermediate nodes. As a result, hostile nodes may get access to the network and disrupt the routing process. Koul et al. [16] suggested a paradigm for deploying security in MANETs while considering specific QoS concerns. The suggested model is multilayered. The MANET is susceptible to various attacks like flooding attacks [17-19], Jellyfish (JF) attacks, jamming attacks, etc.

Flooding is a DoS attack that uses many fake packets and messages to decrease network resources. Flooding assaults come in various forms, the most common of which is a request [20-22]. The request flooding assault continues to saturate the network with requests to fake nodes that don't exist. AIF AODV, an upgraded AODV method that can identify and segregate flooding nodes in a network, was introduced by Abu Zant et al. [23].

The Jellyfish assault is a sort of DoS attack that is difficult to detect due to its dynamic behaviour. A MANET approach for detecting jellyfish attacks [24]. The suggested technique for detecting jellyfish attacks integrates node authentication and trustworthiness with the KNN algorithm. Each node generates trust values based on nearby node recommendations to find the attacker node. The suggested technique would then use nodes' hierarchical trust assessment attribute to select dependable nodes for packet routing. Insider jamming assaults in MANETs can be detected and mitigated using a unique reputation-based coalition game [25]-[29].

3. The Proposed TBR Technique

3.1. Structure of the System

The cluster structure was employed for reliability management, evaluation, and secure routing in the trust-based model method suggested in this research. The trust management node (TMN) and the trust agent node (TAN) are used to assess and manage node dependability. The TMN is in charge of monitoring and reporting on the nodes in each cluster's reliability. While supporting the TMN, the TAN collects the dependability of each neighbour node. This study proposes a trust-based model security routing (TSR) technique that consists of three phases: managing trust, safe path, and safe data transmission. To begin, the TMN saves the node reliability values obtained by the trust agent in all clusters and periodically stores the neighbour TMN and reliability information. The traffic received from neighbour nodes is utilised to identify whether the traffic originated or was routed by the neighbour nodes. On a routine basis, the mean reliability value for the cluster's nodes is determined. Traffic measurements along a predetermined path are also used to find anomaly nodes shown in Fig. 1.

For effective trust evaluation and administration of nodes, the proposed system uses a hierarchical cluster topology in this research. The TMN is the node in each cluster with the greatest connections to other nodes, which manages the nodes' dependability values. Furthermore, the Member Trust Table (MTT), which stores reliability, is stored regularly while sharing data with the TMN of the next cluster. When choosing a route, the average reliability rating is calculated regularly and utilised as a security threshold value. To determine the reliability of nodes inside each cluster, all nodes that act as trust agents are employed. To put it another way, the proportion of packets forwarded by each node determines reliability. The reliability may not be adequately quantified if the delivery of packets is employed. This is because the pace of packet transmission might rise for various reasons, including an increase in traffic, a change in the wireless network's communication state, or a malicious attack.

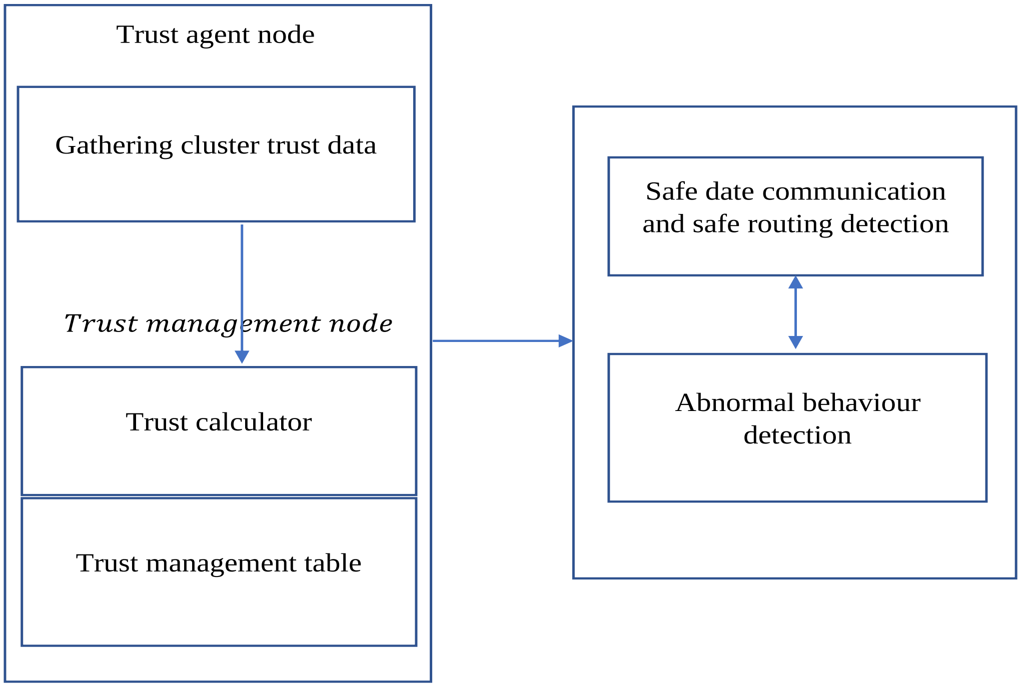
Trust agent node
Gathering cluster trust data
Trust management node
Trust calculator
Trust management table
Safe date communication and safe routing detection
Abnormal behaviour detection

Fig. 1 Structure of the system

As a result, the accuracy of dependability assessment is improved by reflecting the quality of packet forwarding. The information of packets received from a neighbour node is evaluated in order to determine a node's dependability. It is given by

$$T(i) = \alpha \frac{F_i\,(P_j)}{G_i\,(P_i)} + \beta \frac{F_i\,(D_j)}{G_i\,(D_i)} \qquad (1)$$

The trust information table (TIT) in the TMN stores dependability data for every node in the network. Nodes H and S evaluate the value of node A's reliability by storing packets delivered from node A by neighbours. The following equation is used to recalculate the reliability value as:

$$T(K) = avg(\textstyle\sum_{i=o}^{n} T_i(K)) \qquad (2)$$

After all nodes' reliability values have been obtained, the cluster's reliability average value is calculated on a regular basis in the TMN of each cluster using eqn (3). C_i stands for the cluster numbers that make up the network, and it's an expression for computing each cluster's average reliability:

$$C_i T(K) = \frac{\sum_{i=o}^{n} N_i T(K)}{N+1} \qquad (3)$$

The source node sends $RREQ$ signal to set the route to the destination node (D). There are numerous options ranging from S to D. Because the nodes' reliability levels are lower than the cluster's, they are not included in the route setting.

3.2. Data Transmission Techniques for Security

After establishing a secure route between S and D, the key exchange mechanism is employed for secure data transfer in the approach described in the preceding section. For safe path setup, it establishes the path depending on the nodes' dependability check. Because malevolent nodes cannot be excluded through this method, this is used to improve the integrity and security of data exchange. Furthermore, without the assistance of a CA for certificate issuance, key exchange between nodes provides a rapid security function. The TMN sends each node its dependability information regularly. To avoid node falsification, the data is signed by the public key shared between TMNs. This data is used to verify its identity during key exchange to ensure secure data transport. The following is the procedure for exchanging keys between nodes. The source node delivers its hash signature and common key to nodes on a safe route for safe information transfer. The packet's destination node sends a response notification containing a public key and the public key's Integrity Detection Code (IDC). The data is subsequently encrypted and delivered. This technology improves the security and integrity of data transfers.

3.3. Anamoly Detection

Malevolent nodes in the network degrade the routing method's performance. This section follows the procedure to find anomaly nodes in the routing method. The secure path module first discovers a problematic node by checking its traffic. A DSN check in the node's path table entry identifies the rogue node. For the next t hours, the traffic will be monitored. The t value is calculated using the Round Trip Time (RTT) between S and D, and the mean traffic value is found by:

$$t = \frac{1}{RTT\sqrt{\frac{2B}{3}p}} + \frac{1}{T_0 \min\{1,3\sqrt{\frac{3B}{8}p}\}p(1+32p^2)} \qquad (4)$$

Algorithm 1. Anomaly node identification using DSN analysis on the path

```
    1. Examine the amount of traffic (T) between the source and destination nodes.
    2. Using TMN, compute average cluster traffic.
    3.If Cluster average < T
    4. Examine the DSNs of the nodes in the path.
    Else
    Repeat from step 2
    5. Send unusual node information to the TMN.
```

4. Experiments and Results

The outcomes of the proposed TSR technique suggested are evaluated in this part. NS2 is used to run the simulations. Table 1 shows the simulation parameters.

Table 1. Parameters used for the simulation

Parameter	**Values**
Time taken for simulation	600
Maximum speed	0~20 m/s
Number of nodes	50
MAC protocol	IEEE 802.11 DCF
Traffic rate	10 packets/sec
Packet size	512 bytes
Mobility mode	Random waypoint
Network size	1000 m × 1000 m

4.1. Average Delay

As stated and illustrated in Figure 2, it is computed by deducting the delays for all nodes sent from the number of packets found.

$$\text{Average Delay}=\frac{Sum\ of\ all\ packets\ Delay}{Total\ No.of\ Received\ Packets} \qquad (5)$$

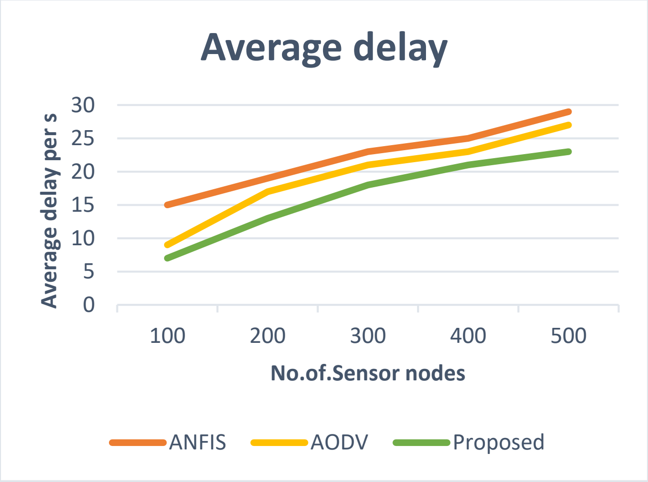

Fig. 2 Average delay comparison

4.2. Throughput

In most circumstances, throughput is calculated in bits per second and expressed as an average (bps). Throughput is lowered due to the high rate of unsuccessful message transmission. Throughput determines how efficiently packets are distributed from one network to another. The entire amount of data transmitted in a particular time is throughput. In Eq (6) throughput, D_p denotes the submitted packets number, and P_s indicates the size of a packet shown in Fig. 3.

$$Throughput = \frac{D_p \times P_s}{Total\ Number\ of\ Internal} \qquad (6)$$

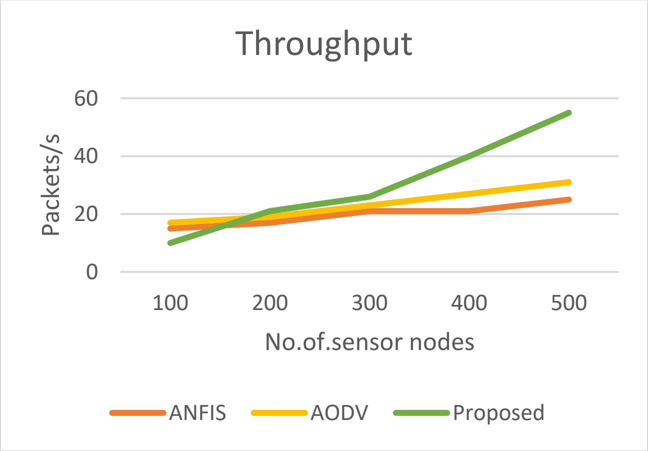

Fig. 3 Throughput

4.3. Packet Loss

It occurs when data packets do not reach the destination node for a variety of causes, including packet dropping, data transmission errors, and network congestion caused by heavy loads shown in Fig. 4.

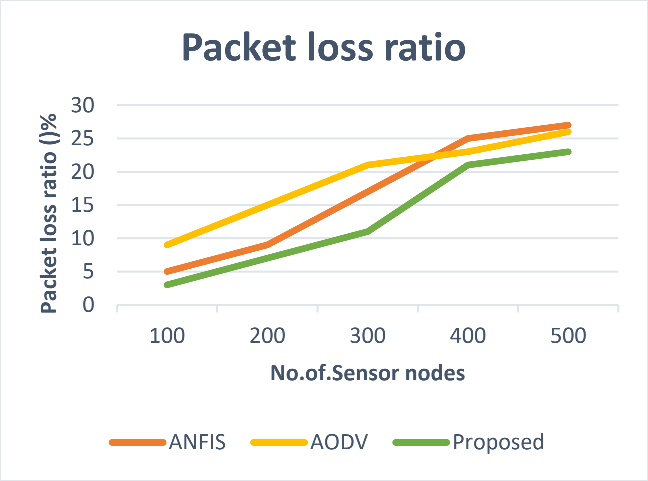

Fig. 4 Packet loss ratio

4.4. Packet Delivery Ratio (PDR)

PDR is the measure of the amount of packets sent by the source node to the amount of packets received by the destination node.

$$\text{Packet delivery ratio} = \frac{\textit{Received Packets}}{\textit{Send packets}} \times 100 \qquad (7)$$

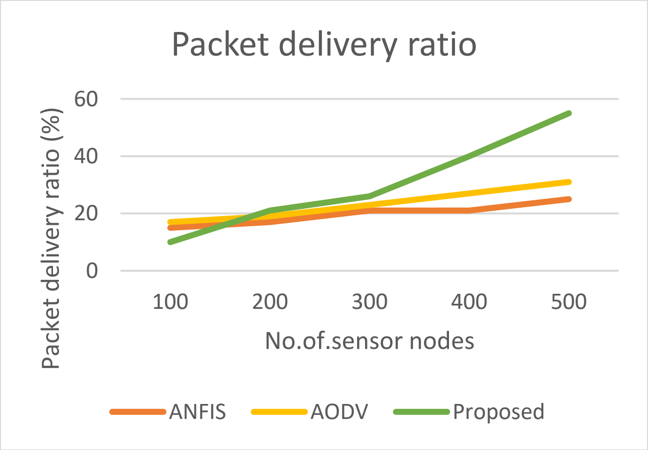

Fig. 5 PDR during the presence of hello flooding attacks

Fig. 5 depicts the PDR measurement results, which is the routing protocol's major performance evaluation criterion. The AODV approach performed poorly in the Hello flooding attack. After conducting $RREQ$ and $RREP$ authentication for route discovery, this technique sets the path, and no specific secure technique is used when the data is delivered. As a result, the performance was severely hampered by the Hello flooding assault, which continued to function normally until the path was defined. On the other hand, the suggested approach performed admirably in the attack because data transfer occurs, followed by the source and destination nodes exchanging keys, even after the path has been defined.

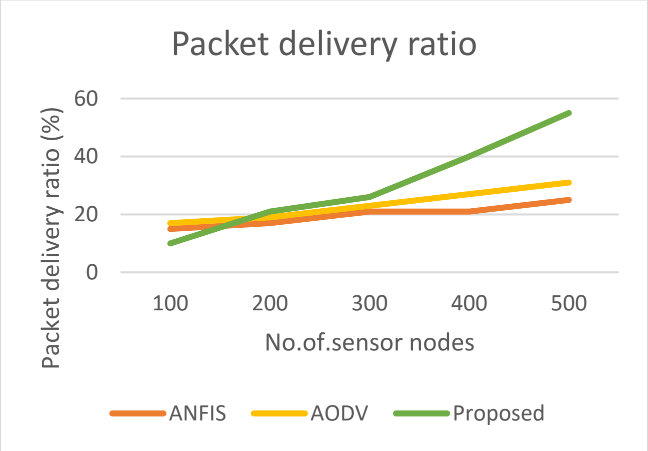

Fig. 6 PDR during the presence of Jellyfish attacks

Fig. 6 illustrates the outcome of confirming the effect of the Jamming attack on packet delivery. As the results demonstrate, AODV's performance in the event of a Jellyfish attack was poor. The proposed technique can achieve good results even in the face of a jamming assault.

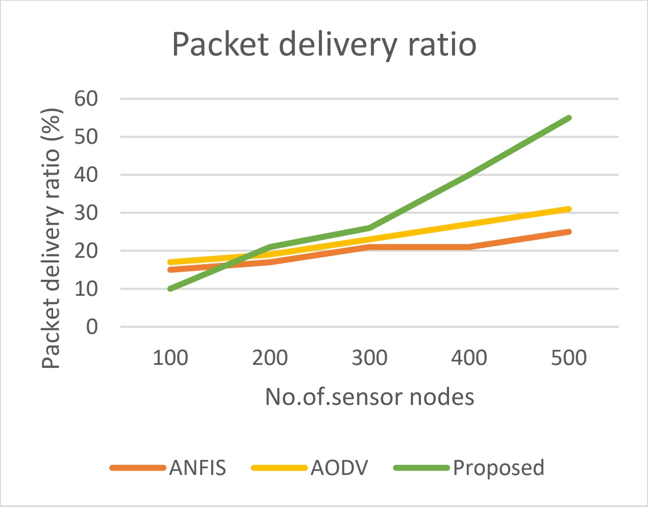

Fig. 7 PDR during the presence of Jamming attacks

The outcome of testing the PDR in the event of a Jellyfish assault is shown in Figure 7. The results reveal that the AODV's performance during the Jellyfish attack was not good. It has been established that the performance of the Jellyfish attack when executing a usual event until the path is set is severely hampered.

Fig. 8 demonstrates the results of the communication delay time between the source and destination nodes. For safe routing, the AODV approach employs TTL values and RREQ and RREP digital signatures.

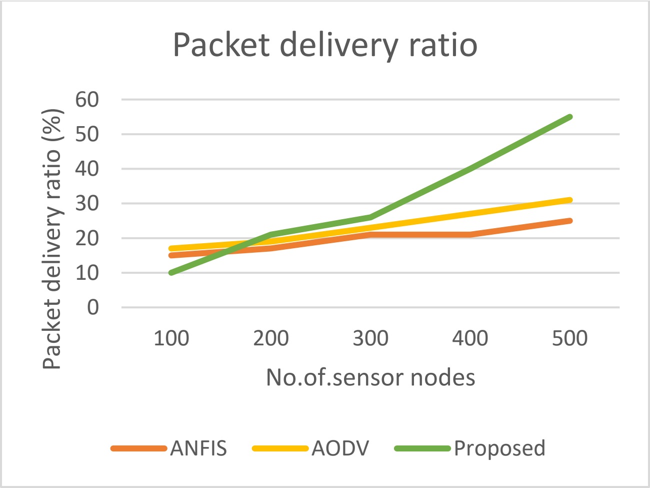

Fig. 8 Results of transmission delay time

5. Conclusion

Because MANET is made up of mobile nodes with limited resources, the routing protocol is crucial in determining overall network performance. Many security vulnerabilities are posed by dynamic topology caused by node mobility and path setup on a hop-by-hop basis. This research proposes a node trust evaluation approach based on cluster structure and a trust-based model security routing (TSR). To improve the efficiency of node reliability evaluation, the proposed technique used a hierarchical structure. Because it assures node reliability evaluation, path establishment between nodes, and safe data exchange, the proposed method in this research can maintain its performance in the presence of hostile nodes. The integrity of data transfer is increased via node-to-node key exchange without CA. The suggested trust-based model security routing strategy outperformed the existing methods in all means of performance measures.

Acknowledgements

The author would like to express his sincere gratitude to the supervisor for his direction and ongoing assistance during this study.

References

[1] K. Sumathi, and A. Priyadharshini, “Energy Optimization in Manets using on-Demand Routing Protocol,” *Procedia Computer Science*, vol. 47, pp. 460-470, 2015.

[2] M. Malathi, and S.Jayashri, “Robust against Route Failure using Power Proficient Reliable Routing in MANET,” *Alexandria Engineering Journal*, vol. 57, no. 1, pp. 11-21, 2018.

[3] S.Chavhan, P. Venkataram, “Emergent Intelligence Based Qos Routing in MANET,” *Procedia Computer Science*, vol. 52, pp. 659-664, 2015.

[4] A.Koul, and H.Kaur, “Quality of Service Oriented Secure Routing Model for Mobile Ad Hoc Networks,” in Proceedings of the 2017 *International Conference on Intelligent Systems, Metaheuristics& Swarm Intelligence*, pp. 88-92, 2017.

[5] S. N. Shah, and R. H. Jhaveri, “A Trust-Based Scheme Against Packet Dropping Attacks in Manets,” in 2nd *International* Conference on *Applied and Theoretical Computing and Communication Technology*, iCATccT, pp. 68-75, 2016.

[6] R. H. Jhaveri, N. M. Patel, D. C. Jinwala, J. H. Ortiz, and A. P. de la Cruz, “A Composite Trust Model for Secure Routing in Mobile Ad-Hoc Networks,” *Ad Hoc Networks*, vol. 2, pp. 19-45, 2017.

[7] G. Singal, V.Laxmi, M. S. Gaur, S. Todi, V. Rao, M. Tripathi, and R.Kushwaha, “Multi-Constraints Link Stable Multicast Routing Protocol in Manets,” *Ad Hoc Networks*, vol. 63, pp. 115-128, 2017.

[8] Y. M. Khamayseh, S. A. Aljawarneh, and A. E. Asaad, “Ensuring Survivability Against Black Hole Attacks in MANETS for Preserving Energy Efficiency, Sustainable Computing,” *Informatics and Systems*, vol. 18, pp. 90-100, 2018.

[9] P. S. Rajendra Prasad, “Efficient Performance Analysis of Energy Aware on Demand Routing Protocol in Mobile Ad-Hoc Network,” *Engineering Reports*, vol. 2, no. 3, pp. 1-14, 2019.

[10] N. M. Quy, N. T. Ban, and V. K. Quy, “An Adaptive on-Demand Routing Protocol with Qos Support for Urban-Manets,” *IAENG International Journal of Computer Science*, vol. 49, no. 1, pp. 1-8, 2022.

[11] R. K. Sahu, and N. S. Chaudhari, “Energy Reduction Multipath Routing Protocol for MANET using Recoil Technique,” *Electronics*, vol. 7, no. 5, pp. 56, 2018.

[12] H. H. Choi, and J. R. Lee, “Local Flooding-Based on-Demand Routing Protocol for Mobile Ad Hoc Networks,” *IEEE Access*, vol. 7, pp. 85937-85948, 2019.

[13] H. N. Saha, and P.Mitra, “Intelligent Energy Aware Fidelity Based on-Demand Secure Routing Protocol for MANET,” *International Journal of Computer Network & Information Security*, vol. 10, no. 4, pp. 48-64, 2018.

[14] S. K. Duvvuri, and S.Ramakrishna, “Adaptive Neuro-Fuzzy Inference System Based on-Demand Fault Tolerant Routing Protocol (ANFIS-ODFTR) for Manets,” *International Journal of Computer Networks and Applications*, vol. 8, no. 6, pp. 719-729, 2021.

[15] R. Hinge, and J. Dubey, “Opinion Based Trusted AODV Routing Protocol for MANET,” in Proceedings of the *Second International Conference on Information and Communication Technology for Competitive Strategies*, pp. 1-5, 2016.

[16] A. Koul, and H.Kaur, “Quality of Service Oriented Secure Routing Model for Mobile Ad Hoc Networks,” In Proceedings of the *International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence*, pp. 88-92, 2017.

[17] S. Gurung, and S.Chauhan, “A Novel Approach for Mitigating Route Request Flooding Attack in MANET,” *Wireless Networks, vol.* 24, no. 8, pp. 2899-2914, 2018.

[18] H. Ehsan, and F. A. Khan, “Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs,” in 2012 IEEE 11th *International Conference on Trust, Security and Privacy in Computing and Communications,* pp. 1181-1187, 2012.

[19] P. Choudhury, S. Nandi, A. Pal, and N. C. Debnath, “Mitigating Route Request Flooding Attack in MANET using Node Reputation,” in *IEEE 10th International Conference on Industrial Informatics*, pp. 1010-1015, 2012.

[20] V. Laxmi, D. Mehta, M. S. Gaur, P.Faruki, and C. Lal, “Impact Analysis of JellyFish Attack on TCP-based Mobile Ad-Hoc Networks,” in Proceedings of the *6th International Conference on Security of Information and Networks*, pp. 189-195, 2013.

[21] B. P. Pooja, M. P. Manish, and B. P. Megha, “Jellyfish Attack Detection and Prevention in MANET,” in 2017 *Third International Conference on Sensing, Signal Processing and Security (ICSSS),* pp. 54-60, 2017.

[22] D. Bhawsar, and A. Suryavanshi, “Collaborative Intrusion Detection and Prevention Against Jellyfish Attack in MANET,” *International Journal of Computer Applications*, vol. 129, no. 13, pp. 37-42, 2015.

[23] M. Abu Zant, and A.Yasin, “Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol AIF_AODV,” *Security and Communication Networks,* vol. 2019, pp. 1-13, 2019.

[24] Z. A. Zardari, J. He, M. S.Pathan, S. Qureshi, M. I. Hussain, F.Razaque, and N.Zhu, “Detection and Prevention of Jellyfish Attacks Using KNN Algorithm and Trusted Routing Scheme in Manet,” *International Journal of Network Security*, vol. 23, no. 1, pp. 77-87, 2021.

[25] A. Al Sharah, T. Oyedare, and S. Shetty, “Detecting and Mitigating Smart Insider Jamming Attacks in Manets Using Reputation-Based Coalition Game,” *Journal of Computer Networks and Communications*, vol. 2016, pp. 1-14, 2016.

[26] K. Manojkumar, S. Devi, "Jamming Attack in Wireless Sensor Networks using Ant Colony Algorithm," *SSRG International Journal of Computer Science and Engineering,* vol. 8, no. 2, pp. 6-9, 2021. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V8I2P102

[27] M.Supriya, Dr.T.Adilakshmi, "Secure Routing using ISMO for Wireless Sensor Networks," *SSRG International Journal of Computer Science and Engineering,* vol. 8, no. 12, pp. 14-20, 2021. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V8I12P103

[28] S Yasaswini, G.M.Naik, P G K Sirisha, "Efficient Loss Recovery in Ad Hoc Networks," *SSRG International Journal of Computer Science and Engineering,* vol. 4, no. 1, pp. 1-7, 2017. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V4I1P101

[29] Nelesh Sharma, Dr. NirupamaTiwari, "Implementation of Multipath AODV for Enhanced Performance in Wireless Ad hoc Network," *SSRG International Journal of Computer Science and Engineering,* vol. 6, no. 9, pp. 15-19, 2019.
Crossref, https://doi.org/10.14445/23488387/IJCSE-V6I9P104.