IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE ROUTING PERFORMANCE USING TRUST MODEL IN MANET

K.Divya[1] and Dr. B.Srinivasan[2]

[1]Ph.D Research Scholar, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, INDIA

[2]Associate Professor, Gobi Arts & Science College, Gobichettipalayam, INDIA

Abstract: MANET is utilized in many fields because of its advantage in quickly establishing networks. The network will perform well if mobile nodes trust each other and act cooperatively. However, dynamic topology characteristics and frequent connection failures by the movement of nodes make routing difficult and cause vulnerability to be easily exposed. Therefore, the routing provided in the MANET should have security features that can reduce the damage to various attacks. For this, in this paper, it is proposed for a trust evaluation method of nodes using cluster structure and a secure data transmission technique through key exchange without CA. The proposed technique adopted a hierarchical structure to enhance the efficiency of the reliability evaluation of nodes. The reliability measurement reflects the quality of packets as well as the number of packets and the measured reliability is maintained by the trust management node. The integrity of the data transmission is improved through key exchange without CA between the nodes. In order to increase the efficiency of routing, anomaly nodes are detected by DSN checking of nodes that generate excessive traffic on the path when data is transmitted.

Index Terms – **MANET, Routing Protocols, Trust based, DSR, SAODV.**

- **Introduction**

MANET is a network consisting of only mobile nodes without a fixed infrastructure. It does not require a wired network, access point, and base station in the process of configuring the network. The mobile nodes composing MANET do not only perform the transmission and reception of data that the existing host performs but also act as routers. In route settings, it can support multipathing to neighbor nodes and perform routing dynamically because the mobile nodes act as routers. However, it is exposed to many security vulnerabilities due to the nature of the dynamic topology and the wireless network by the movement of nodes. However, there is a problem that the number of control packets increases in order to maintain the routing to the destination. Also, it has been studied on various routing attacks by malicious nodes. In order to cope with such a routing attack, the technique that uses the reliability of mobile nodes participating in routing or involves authentication nodes to routing by issuing certificates to mobile nodes has been studied.

In this paper, we propose a trust model-based secure routing technique to improve the efficiency of the trust evaluation and the performance of secure routing problem of security routing in the existing studies. This technique consists of the trust evaluation step and security routing step. In the trust evaluation step, a hierarchical structure is applied to increase the efficiency of the reliability measurement for each node. In the security routing step, the security communication function through the routing based reliability and key exchange is provided in order to security routing performance.

The proposed technique uses cluster hierarchy to improve the reliability evaluation efficiency. The reliability evaluation is performed by measuring the packet forwarding rate of the neighbor nodes of all nodes. The trust management node manages the measured reliability of the mobile nodes in each cluster and the measured reliability is used to set a route between the source and destination node. For secure data communication, the key generation and exchange between nodes without the help of Certification Authority (CA) is applied.

In this way, the key generation process is simplified, and the processing speed can be improved while improving the communication data. Also, the traffic on the route is checked to detect anomaly node on the path. If the traffic on the route is higher than the average traffic in the cluster, it checks the DSN of the intermediate nodes existing between the source node and the destination node and detects an anomaly node that transmits a packet to a node using a wrong DSN or a node ID that does not exist. The improved performance of the trust based model security routing technique proposed in this paper is confirmed by minimizing routing efficiency and the number of control packets through performance analysis experiments with SAODV based the proposed simulation parameters and performance metrics.

- **Related Research**

2.1 Routing Protocols

The routing protocol in MANET can be classified into table-driven routing protocols using the Bellman–Ford algorithm and hybrid method that combines the advantage of table-driven routing protocol and on-demand routing protocol. The table-driven routing protocol is a method to maintain the latest network information by storing the entire path for all nodes in each entry of the table and broadcasting routing information periodically or when the network topology changes. When there is a connection request due to traffic occurrence, it has a benefit that connection setup is fast because of having the path information. But, it has a problem that the broadcasting overhead of the control message for path management is large and resources are consumed for discovering a path that is not used for frequent phase changes. The routing protocols of this type include Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), and Source Tree Adaptive Routing (STAR).

First, the source routing method is that a transmitting node calculates routing information for transmitting data and the data including the routing information in the header is transmitted to the destination. Link Quality Source Routing (LQSR) is a typical protocol. The intermediate node only refers to the information of the header and delivers to the next node. But the payload of the frame is reduced. Second, the hop-by-hop routing method is that all nodes have all information of the next hop for delivering to the destination. The immediate node delivers frame to the next hop of its routing information by referring to the destination information of the header. There is less overhead because it is a simple method. The on-demand routing protocol does not always maintain the full path for all mobile nodes, but the path gain procedure is performed when data transmission is required. This means that a routing table to a destination node is generated after performing a path search process only when data transmission is required.
In addition, if the path to the destination node cannot be searched, problems such as a broadcast storm can be caused because a message requesting the path continuously is generated until the path is searched. Thus, on-demand routing protocol focuses on minimizing the optimal path search and delay time of the path search. These routing protocols include Dynamic Source Routing (DSR), Ad Hoc On-Demand Distance Vector (AODV), and Dynamical MANET On-Demand Routing (DYMO). Hybrid routing protocol is a method of mixing proactive and reactive methods. This performs mixed routing that proactive method is used for nodes in the environment where there is little change in topology due to small movement of nodes and the reactive method is used where the nodes are frequently moved.

Table 1 Difference between source routing and hop-by-hop routing

Routing	Key features
Source routing	Sending node calculates routing information The intermediate node only refers to the information of the header and delivers to the next node Advantages of the reduced frame payload
Hop-by-hop routing	All nodes have all information of the hop to the destination The immediate node delivers frame to the next hop of its routing information Less overhead in a simple way

Table 2 The characteristics of the routing protocol

	Proactive	Reactive	Hybrid
Routing technique	Nodes send periodic messages to keep up-to-date routing information in the table	Perform routing by requesting routing information only when sending and receiving data	Mix proactive and reactive advantages
Advantage	Minimize delay for routing	Minimize routing overhead	Expand the scope of application by combining the advantages of two methods
Disadvantage	Routing overhead increases	Routing latency increases	The protocol is complex

Energy-Aware AODV (EAODV) utilizes backup routing techniques based on AODV. Since this technique sets a path in consideration of the remaining energy of a node, it can reduce link errors due to energy exhaustion and the network can be maintained for a long time. PS-AODV is a technique for determining routing based on a load situation between nodes. The node first checks the current load before forwarding the RREQ packet for route discovery to neighbor nodes. The RREQ packet is discarded if the node load is very high. Subsequently, if the load of the node decreases, the next RREQ packet is forwarded again.

2.2 Routing Attacks

Routing attacks can be divided into passive attacks which can cause a lot of damage through the eavesdropping or tapping of packets, and active attacks which prevent routing or make packet transmission impossible by inserting, discarding, or modifying incorrect information in the routing process. The typical attack among these routing attacks includes the black hole attack, wormhole attack, Jellyfish attack, and Sybil attack.

The black hole attack is an attack in which an attack node changes route by sending incorrect routing information to the source node. In other words, it is an attack which intercepts all packets to be transmitted to the destination node by analyzing RREQ packet for route discovery and transmitting RREQ as if the shortest route to the destination node is itself to the source node. The wormhole attack has two ways. One is to eavesdrop on data packets that two attack nodes trick as if the neighbor nodes are close to each other and the route formed by the two nodes is optimal.

The Sybil attack is an attack in which the attack node generates multiple IDs and makes other nodes be recognized as multiple identifiers. It is very threatening to the routing method using geographic information. Jamming attack is a type of denial of service attack that is detrimental to the reliability of wireless communication. This attack interferes with communication between nodes and causes data transmission failure by transmitting any meaningless signal to the corresponding wireless channel.

2.3 Secure Routing Method

Secure Ad Hoc On-Demand Vector (SAODV) as a typical routing technique in MANET uses digital signatures for RREQ and RREP authentication and authenticates hops using hash chains. First, a maximum number of hops are set and a one-way hash function with one greater than the number of hops is created. Then, the RREQ transformed by the hash function is created and transmitted. The nodes receiving the RREQ authenticate the RREQ packet and the RREQ is created and transmitted in the same way if it is correct.

Secure Energy-Efficient Routing (SEER) authenticates data using a one-way hash chain and uses a shared secret key between the mobile node and the base station to improve confidentially. This technique creates a tree based on the base station and initializes the one-way hash chain. Feedback based secure routing protocol (FBSR) is an energy efficiency-oriented routing protocol using evaluation functions. This technique provides security by using a one-way hash function which is authentication of the MAC layer. The evaluation function uses a combination of energy level and distance, and the energy level is used by the threshold evaluation function. This technique provides two methods to prevent routing attacks. First, the feedback from the neighbor nodes is signed by one-way hash chain. The second is to utilize feedback to base station in order to distinguish attack nodes.

2.4 Trust Based Routing Protocol

In MANET, secure routing protocol has been studied for various ways that utilize key management, encryption, or continuous monitoring of neighbor. However, most of these methods have the disadvantage that these are too costly for secure routing and are not suitable for the proposed MANET. This is performed only when malicious nodes send erroneous information. Each node consumes more memory because it scans and maintains the table periodically. This technique assumes that all nodes have the same frequency range. It is proposed that intermedia node plays a role as a trust gateway maintaining the trust level in order to avoid malicious nodes. The source node calculates the optimal path

by using this trust information. The reliability calculation is based on forwarding behavior of nodes. The trusted gateway node should consume a lot of energy and be less mobile. In TAODV, reliability is determined by the opinion used in the subjective logic.

Trust-Based Minimum Cost Aware (TMCQA) proposes a technique for efficient data collection on the network. This technique uses machine learning to evaluate the trust of data reporter. And a selection strategy of an optimized data reporter based on three key evaluations is used. Trust Detection-Based Secured Routing (TDSR) uses a sensor node to evaluate the trust of an intermediate node for a secure path between a source node and a destination node.

- **The Trust Based Model Secure Routing Technique**

3.1 System Structure

The trust-based model secure routing technique proposed in this paper used the cluster structure for reliability evaluation, management, and security routing. The trust management node and the trust agent node are used for reliability evaluation and management of nodes. The trust management node is responsible for managing the reliability of the nodes in each cluster and providing the information. The trust-based model security routing technique proposed in this paper consists of three modules: trust management module, security path module, and secure data communication module. First, the trust management module stores the reliability value of the nodes collected by the trust agent in each cluster and updates the neighbor trust management node and reliability information periodically. The reliability measurement on nodes is based on the traffic received from the neighbor nodes and checks whether the traffic is packet generated by the neighbor nodes or forwarded. And the average value of reliability for the nodes in the cluster is calculated periodically. Second, the secure path module performs a security routing based on measured reliability when the path is set from the source node to the destination node. The third secure data communication module performs data communication after key exchange between the source node and the destination node for secure data communication. In particular, this key exchange can provide integrity and non repudiation as a technique for providing a security function of a routing protocol without CA assistance.

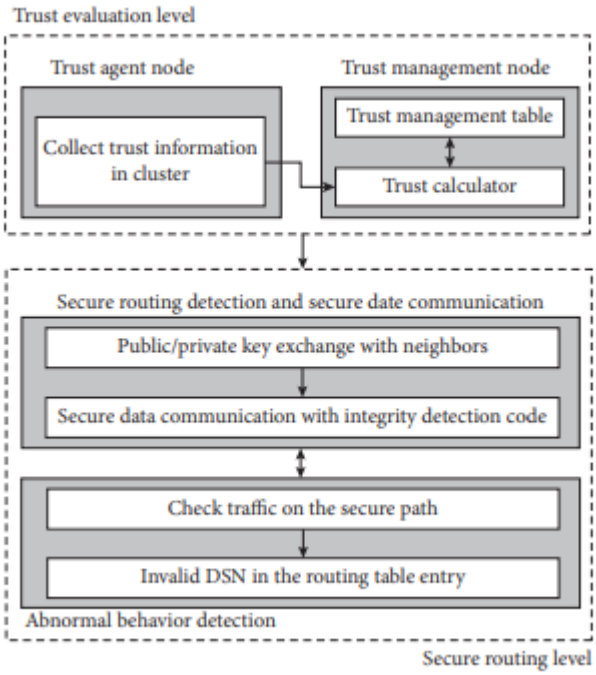

Figure 1 The Trust Based Model routing System Structure

3.2 Reliability Measurement and Security Routing

The node with the highest number of connections with nodes within each cluster is designated as the trust management node, and this node manages the reliability value of the nodes in each cluster. In addition, the Member Trust Table (MTT) storing the reliability is periodically updated while exchanging information with the trust management node of the adjacent cluster. In order to improve security when setting the route, the average value of the reliability is periodically calculated and used as a threshold value. That is, the reliability measurement is calculated using the ratio of packets forwarded by each node. However, the reliability may not be measured accurately if only the delivery of the packets is used. This is because the rate of the packet transmission may increase due to various reasons such as traffic increase, the communication state of wireless network, and malicious attack. In order to measure the reliability of a specific node, the contents of packets received from the neighbor node are analyzed. First, the IP header of the received packet is checked to determine whether the packet is a packet generated by a neighbor node or simply a forwarded packet. Then, the reliability for each node is calculated by the following equation:

$$T(i) = \alpha \frac{F_i(p_j)}{G_i(p_i)} + \beta \frac{F_i(D_j)}{G_i(D_i)}.$$

Here, α and β mean the weight according to the time that node i and node j participate in the network. Gi(pj) means that node j delivers the generated packet to node i, Fi(pj) means that node j is packet delivered to node i packet received from the neighbor node. And Gj(pi) means that node i delivers to node j generated packet, Fj(pi) means that node i is the packet delivered to node j packet received from the neighbor node. *is is a way to measure the selfish behavior of a node and the reliability is decreased if a packet received from a neighbor node does not deliver and only its own data is transmitted.

The reliability value measured by each neighbor node is recalculated by the following equation:

$$T(K) = \text{avg}\left(\sum_{i=0}^{n} T_i(K)\right).$$

In the trust management node of each cluster, the reliability average value of the cluster is calculated periodically after the reliability value for all nodes is measured, and this is calculated by equation

$$C_i T(K) \frac{\sum_{i=0}^{n} N_i T(k)}{N+1}.$$

The source node (S) broadcasts the RREQ message to establish the path to the destination node (D). The nodes that receive this message transmit the packet to the destination node and find the paths to the destination node through the response of RREQ. The source node deletes a node whose reliability is less than the average value of cluster reliability among the various paths to the destination node collected by the response.

3.3 Security Data Transmission Technique

This sets the path based on the reliability check of the nodes for secure path setup. And this is applied to enhance the security and integrity of data transmission because malicious nodes cannot be completely excluded through this process. Also, the rapid security function is provided through key exchange between nodes without CA's help for certificate issuance. Each node receives periodically its own reliability information from the trust management node. . The key exchange between nodes is performed as follows. First, the source node sends its public key and hash signature of the public key to nodes of the set secure path for secure data transmission. The destination node which received the packet transmits a response message including a public key and an Integrity Detection Code (IDC) of the public key.

Node ID	Neighbor node	Trust value	Save_time	Cluster ID
A	H	0.4	07:11:09	C_3
	S	0.9	07:03:42	C_1
C	B	1.9	07:11:09	C_2
	J	0.4	07:12:33	C_2
E	D	0.9	06:58:41	C_3
	H	0.4	07:11:09	C_3

Figure 2 The Structure of Trust Information Table

And the source node encrypts data to be transmitted to the destination node and transmits. This technique improves the safety and integrity of data transmission. The source node requests its trust information from its trust management node as a preparation step for key generation with the destination node. The received trust information is transmitted to the destination together. The destination node which received it identifies the source node through the process of requesting the identity of the node to the trust management node.

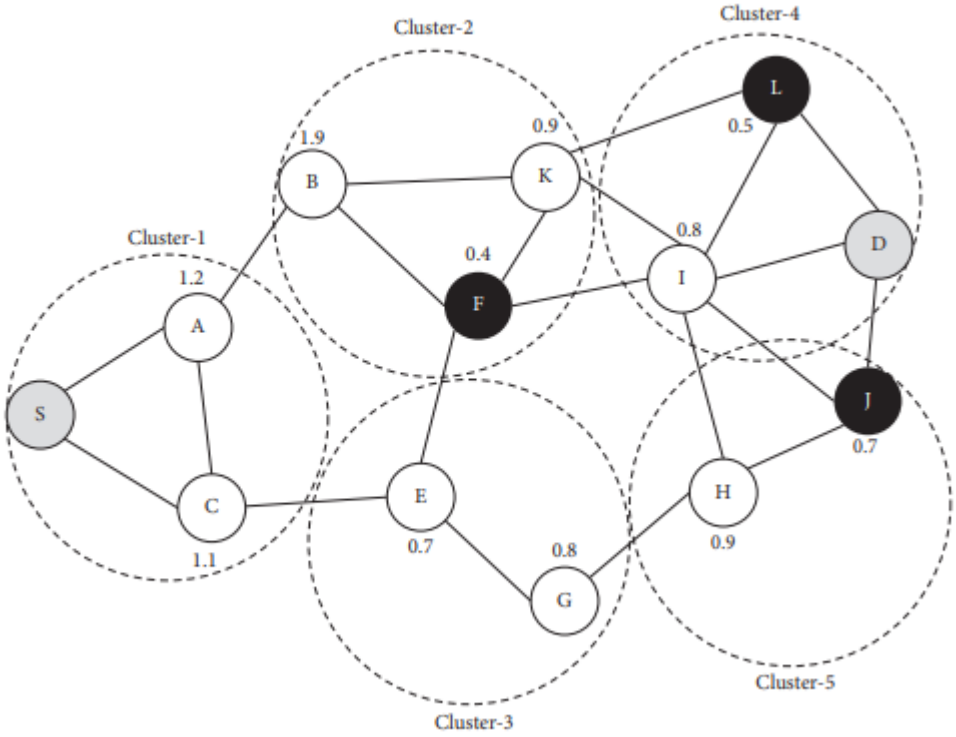

Figure 3 Path setting Flow Diagram based on trust values

- **Experiments and Results**

4.1 Simulation Parameters

The main performance of the trust-based model secure routing technique proposed in this paper. The mobile node used in the experiments is a random waypoint model that changes the location freely while moving the network. In our simulation, the mobile speed is varied 5, 10, 15, and 20 m/s and the battery consumption of the nodes was not considered. The total experiment time was 300 s, and, during the experiment, Hello flooding attack, Jellyfish attack, and Jamming attack occurred 5 times.

4.2 Performance Metrics

The first experiment evaluated security routing performance according to the presence or absence of an attack with SAODV and the second experiment evaluated routing performance according to the network structure with EAODV. The performance evaluation criterion is set as a packet delivery ratio, end-to-end delay time, the number of control packets, network throughput, routing overhead, and average path length.

- Packet delivery ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted
- End-to-end delay time: The end-to-end delay is averaged over all surviving data packets from the sources to the destinations
- Control packet: The number of the total packets, such as RREQ, RREP, and RERR, transmitted for data transfer between the source node and the destination node
- Network throughput: This is a data packet transmitted between a source node and a destination node for a certain period of time
- Routing overhead: The total number of routing packets for route discovery and route maintenance
- Average path length: The average number of hops between the source node and the destination node where data is transmitted

- **Results and Analysis**

The measurement results of the packet delivery ratio, which is the main performance evaluation criterion of the routing protocol. As shown in the figure, we confirmed that the performance difference between the two techniques was not large when the attack did not exist, but the difference was large when the attack did exist. The SAODV technique showed a low performance in Hello flooding attack. This technique sets the path after performing authentication of RREQ and RREP for path discovery, and special secure technique is not applied when the data is transmitted. However, the proposed technique showed excellent performance in the Hello flooding attack because data transmission takes place after performing the key exchange process with the source node and the destination node even after setting the path.

The SAODV technique performs authentication for RREQ and RREP for path discovery and sets the path. The special security technique is not applied when data is transmitted. It is confirmed that the performance is degraded greatly for the Jellyfish attack performing a normal action until the path is set. As the results show, the performance of SADODV was not good in the event of the Jellyfish attack. In the detection of inserted abnormal packets, the performance of packet delivery was degraded because discovery was made after data transmission was completed. On the other hand, the proposed technique can get good results even for Jamming attack due to blocking packet reception from malicious attack node through the process of the key exchange between nodes before data transmission.

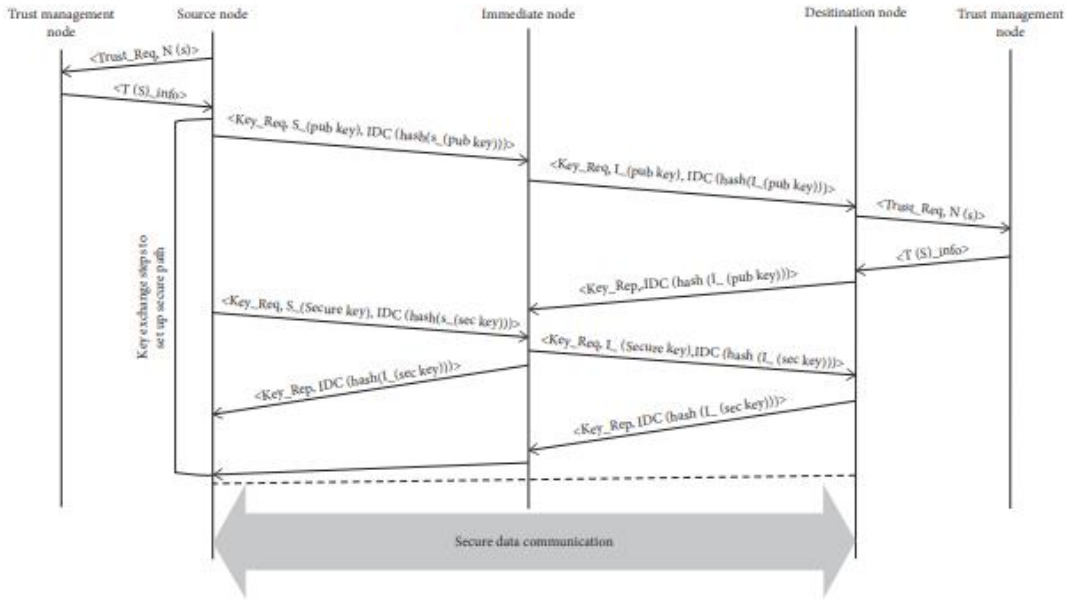

Figure 4 Internodes Key exchange process for secure data transmission

Table 3 Simulation Parameters

Parameter	Value
Number of nodes	50
Simulation time	600
Maximum speed	0~20 m/s
Pause time	5 sec
Transmission range	200m
Network size	1000 m × 1000 m
MAC protocol	IEEE 802.11 DCF
Packet size	512 bytes
Mobility model	Random waypoint
Traffic type	CBR/UDP
Traffic rate	10 packets/sec

The proposed technique is that data is transmitted through a key exchange process even after setting a secure route between the source node and the destination node. Therefore, routing overhead by attacks does not increase significantly although the key exchange occurs.

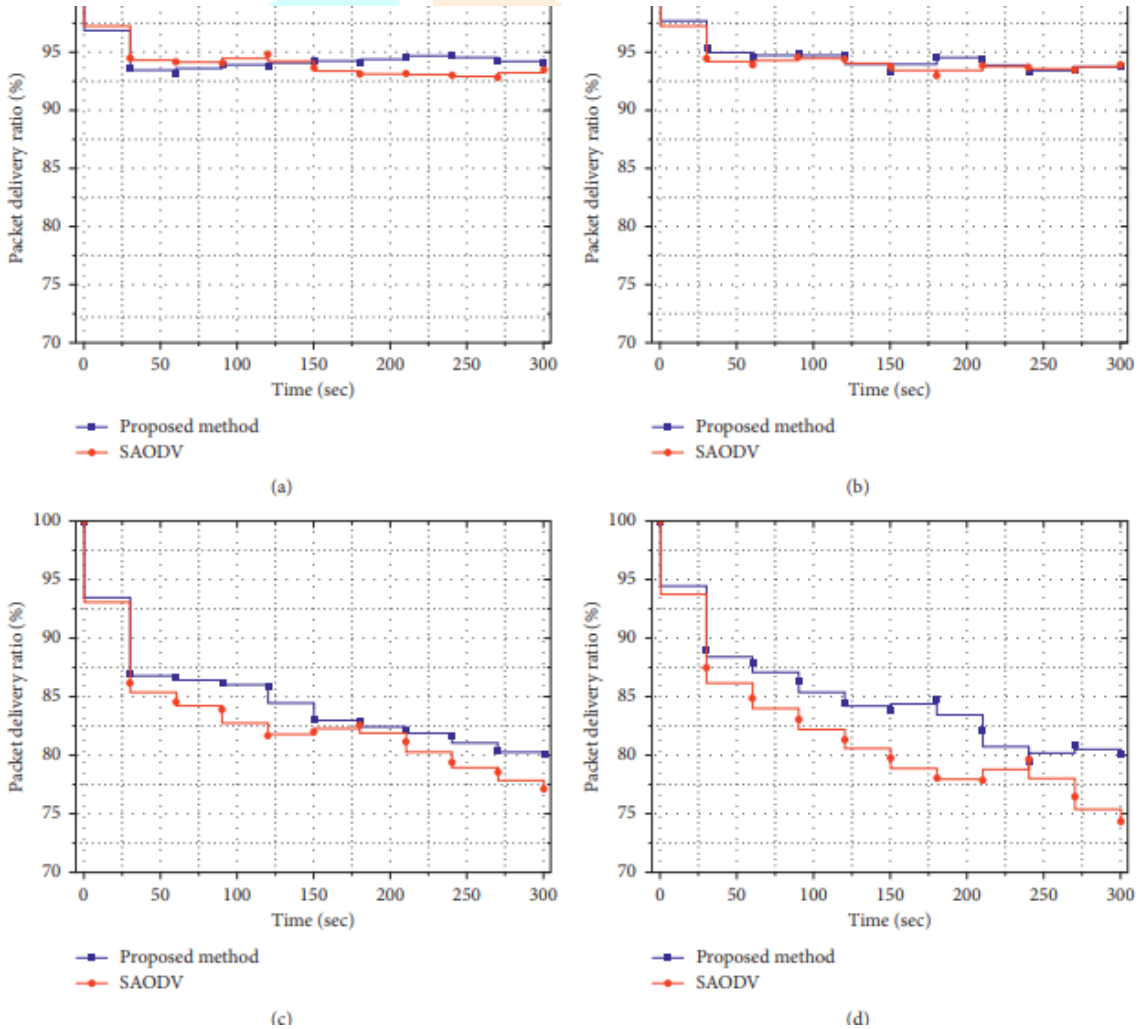

Figure 5 Results of packet delivery rates based on the presence of Hello flooding attacks

The proposed technique selects the shortest path that does not consider residual energy of the node through the path discovery process based on the cluster. Also, the cluster head manages the information of the nodes in the cluster and routes are set based on this. So, more efficient routes are set, but EAODV selects the node with the high energy level,

long path life, and fewer hops. EAODV showed good results when the movement of nodes was less but it showed the lower the result by reflecting the energy threshold calculation as the movement speed of the nodes is faster.

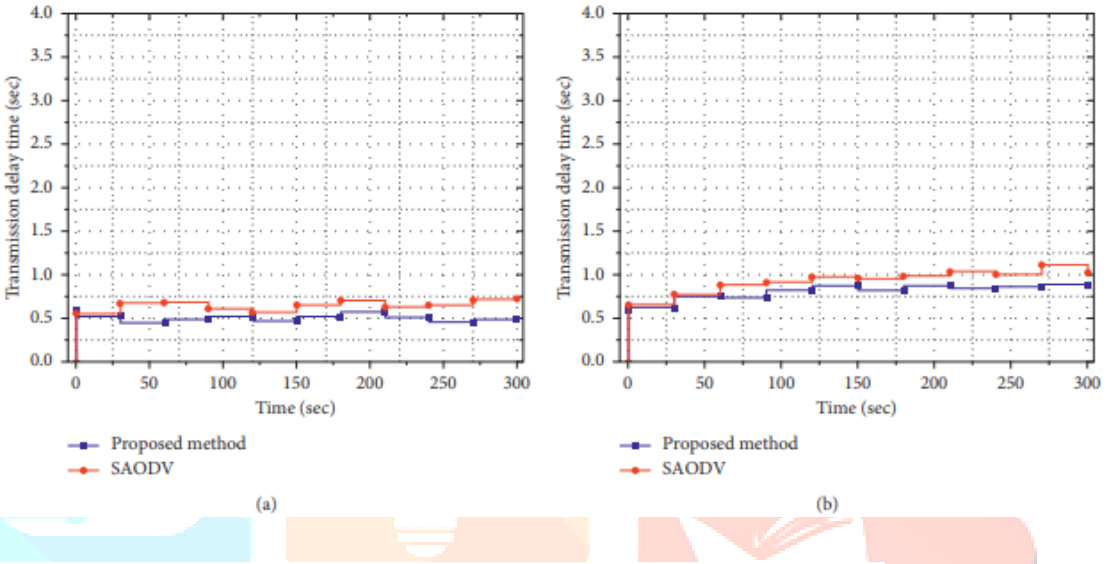

Figure 6 Results of packet delivery rates based on the presence of Jamming attacks.

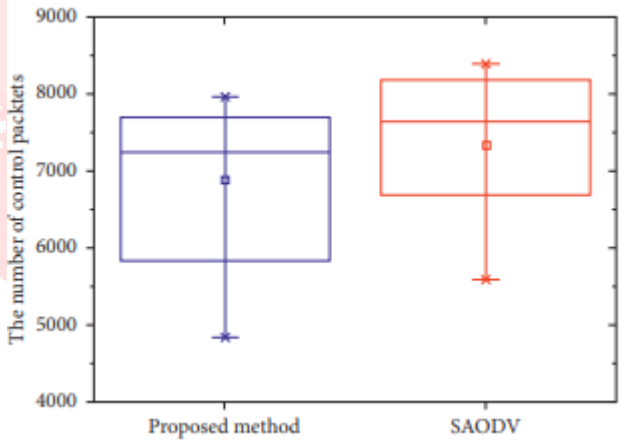

Figure 6 Amount of control packets

As the nodes move faster, the number of routing packets both protocols increases. However, it shows that the routing packet of the proposed technique has fewer routing choices compared to EAODV. Therefore, the number of routing packets for route discovery and maintenance can be reduced.

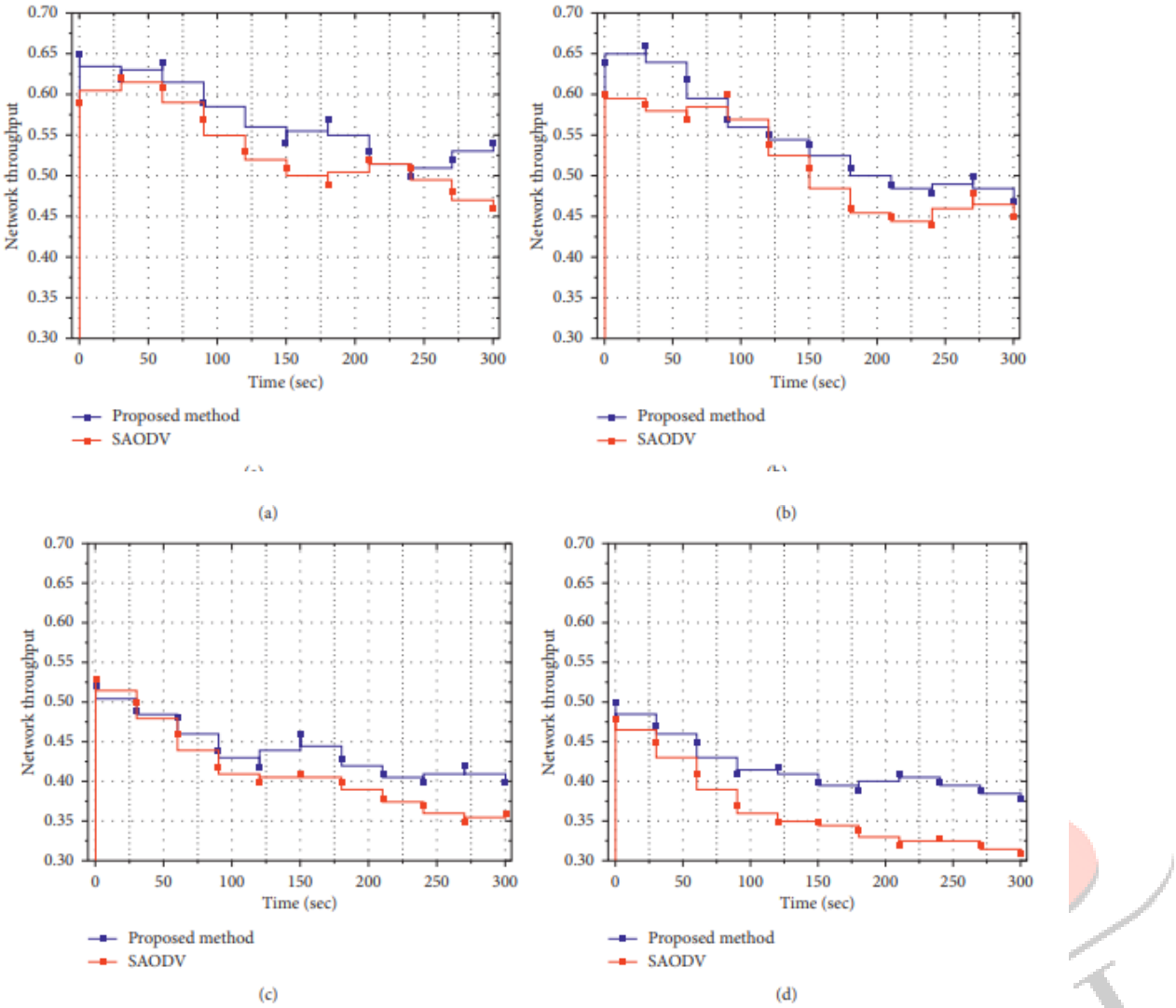

Figure 7 Results of network throughput based on the presence of Jellyfish attacks

- **Conclusions**

The routing protocol plays a very important role in determining the overall network performance because MANET consists of mobile nodes with limited resources. Dynamic topology by the movement of nodes and path setting by hop by-hop provide a threatening cause to many security threats. An internal attack by malicious nodes, especially, is more damaging. It is necessary to provide a technique to eliminate the participation of malicious nodes in routing and data transmission through proper trust evaluation of nodes. For this, the cluster structure was used to measure the reliability of nodes participating in the network in this paper. The reliability information and management of the nodes in each cluster were done by the trust management node. The trust management node calculated the reliability average value of the cluster and transmits the information to the neighbor trust management node every time the reliability value for each node was updated. In this way, even if the nodes move, the trust information of each node can be known. Also, the trust information of each cluster node is digitally signed and transmitted.

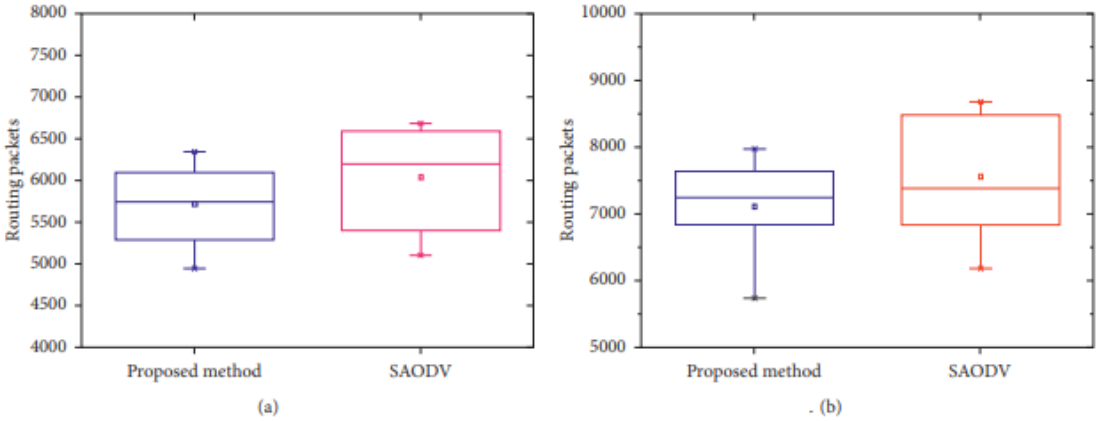

Figure 8 Routing overhead depending on the number of nodes

Among the various paths existing between the source node and the destination node, a node having a value smaller than the reliability average value of the cluster was excluded from the path setting. If the path had been set, the data was transmitted after the key exchange process between the source node and the destination node. The key exchange between nodes was performed without the CA and the trust information received from the trust management node was used to guarantee the identity of the node. We also measured the traffic on the path between the source node and the destination node in order to detect anomaly nodes.

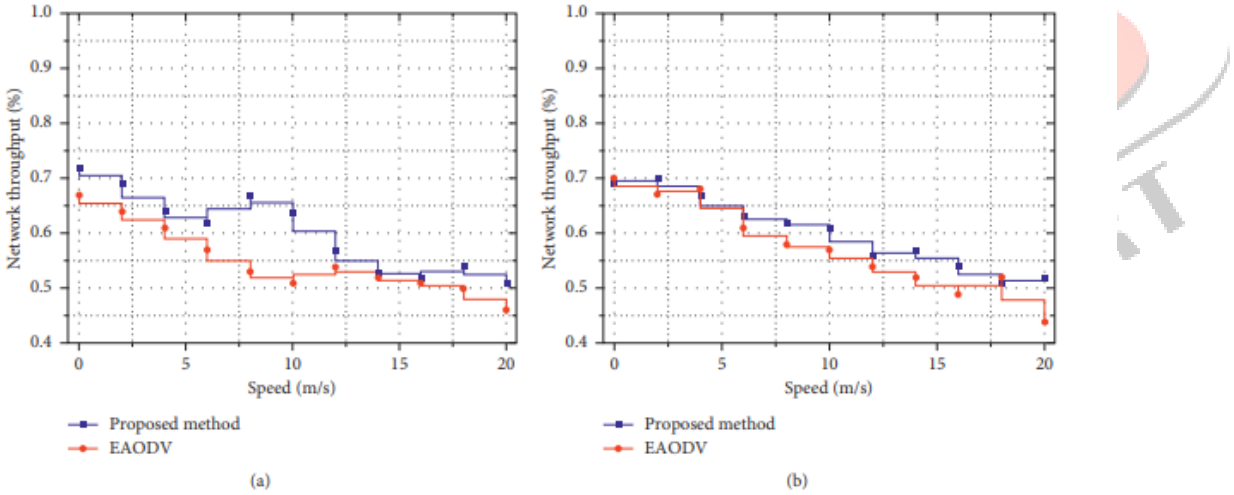

Figure 9 Network throughput depending on number of nodes

In order to evaluate the performance of the proposed technique, the experiment was performed as compared with SAODV technique for packet delivery ratio, end-to-end delay time, the number of control packets, network throughput, and average path length.

Through the experiment, it was confirmed that the management of the nodes and route discovery using a cluster-based network structure is more effective as the moving speed of the nodes increases. As can be seen from the experiment, the better performance of the proposed technique compared to SADOV is confirmed in the presence of the attack. This shows the superiority of the trust evaluation and the security path setting for the proposed nodes.

References

[1] R. Kaur, M . K. Rai, 2012, "A novel review on routing protocols in MANETs," Undergraduate Academic Research Journal (UARJ), vol. 1, no. 1, pp. 103–108.

[2] M. A. Mahdi, T.C. Wan, and R. Abdullah, 2019, "Performance evaluation of MANETs routing protocols in non-uniform node density topology," in Proceedings of the 10th International Conference on Robotics, Vision, Signal Processing and Power Applications, Montreal, Canada.

[3] S. Hemalatha, P. S. Mahesh, 2018, "Energy optimization in directional advanced intruder handling AODV protocol in MANET".

[4] T. Singh, J. Singh, and S. Sharma, 2017,"Energy efficient secured routing protocol for MANETs," Wireless Networks, vol. 23, no. 4, pp. 1001–1009.

[5] K. Mohammadani, 2018, "Stress-based performance analysis of AODV & DSDV routing protocols in MANET".

[6] C. Mbarushimana and A. Shahrabi, 2007, "Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks," in Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), Ontario, Canada.

[7] H. Moudni, M. Er-rouidi, H. Mouncif, and B. El Hadadi, 2016,"Performance analysis of AODV routing protocol in MANET under the influence of routing attacks," in Proceedings of the International Conference on Electrical and Information Technologies (ICEIT), San Francisco, CA, USA.

[8] F.-H. Tseng, H.-P. Chiang, H.-C. Chao, 2018, "Black hole along with other attacks in MANETs: a survey," Journal of Information Processing Systems, vol. 14, no. 1.

[9] C. Del-Valle-Soto, C. Mex-Perera, R. Monroy, NolazcoFlores, and J. Arturo, 2015, "On the routing protocol influence on the resilience of wireless sensor networks to jamming attacks," Sensors, vol. 15, pp. 7619–7649.

[10] Y. Liu, X. Liu, A. Liu, N. N. Xiong, and F. Liu, 2019,"A trust computing-based security routing scheme for cyber physical systems," ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 6, pp. 1–27.