Hindawi
Mobile Information Systems
Volume 2020, Article ID 8819587, 17 pages
https://doi.org/10.1155/2020/8819587

Research Article

A Study on Improving Secure Routing Performance Using Trust Model in MANET

Hwanseok Yang

Department of Information Security Engineering, Joongbu University, Goyang 10279, Republic of Korea

Correspondence should be addressed to Hwanseok Yang; yanghs@joongbu.ac.kr

Received 8 June 2020; Revised 12 August 2020; Accepted 7 September 2020; Published 16 September 2020

Academic Editor: Antonio de la Oliva

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. The proposed technique in this paper can maintain stably the network performance even in the presence of malicious nodes because it ensures reliability evaluation for nodes and the path setting between nodes and secure data transmission. The superior performance of the proposed trust-based model security routing technique was confirmed through comparative experiments for packet delivery ratio, end-to-end delay time, the number of control packets, network throughput, and average path length.

1. 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. It can be constructed quickly at a low cost because there is no restriction on host movement [1–3]. The utilization range of MANET has been used in situations where network configuration is difficult, by the rapid development of wireless networks and the spread of mobile terminals. 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 [4, 5]. 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. In order to solve the problem, various routing techniques for stable data transmission and reception between nodes have been studied. In the existing routing protocol studied, the demand-based AODV protocol has shown excellent performance in various mobility pattern, density, and traffic. 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 particular, if packet loss or route connection failure occurs by various attacks existing on the route, it will take a long time to reconstruct a new path from the source node to the destination node, the number of control packets increases and the resulting overhead is also increased. Therefore, the study on safer and more efficient

secure routing techniques is necessary in order to increase the reliability of MANET [6, 7].

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 main function of the proposed technique is secure data communication through security routing based on reliability evaluation of nodes and the detection of anomaly node through traffic and Destination Sequence Number (DSN) check. 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. The secure routing performance can be improved by excluding the malicious node from participating in the network. 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.

The composition of this paper is as follows. In Section 2 we discuss the kind of routing attacks and secure routing techniques existing in MANET. In Section 3, we describe the trust-based model secure routing techniques proposed in this paper. In Section 4, we verify the performance of the proposed technique through experiments and finally conclude in Section 5.

2. 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 [8–10].

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. Therefore, it is studying to minimize the number of control messages. The routing protocols of this type include Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), and Source-Tree Adaptive Routing (STAR) [11–13].

This routing method can be divided into two different methods according to the method of transferring data. 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. However, loops can occur in the step of setting routing metrics, so a method to avoid this is necessary. Table 1 shows the main characteristics of the two routing techniques.

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. Therefore, there is a disadvantage that the delay time for path discovery is increased. But there is an advantage that the accurate path can be set because the mobility of the mobile node can be reflected immediately when the path is set. 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) [14–16].

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. This can perform efficient routing since this uses a mixture of advantages of the existing methods. But it is not easy to implement and has a complicated operation. Table 2 shows the characteristics of MANET routing techniques.

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. Also, if the energy level of nodes becomes less than the threshold by setting the threshold energy level of nodes, the data loss and transmission delay that occur in case of path change and path resetting can be reduced by transmitting error packets to the source node [17].

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. In this way, the routing considered this will be done because the higher the load of the node is, the more energy is consumed [18].

2.2. Routing Attacks. MANET is vulnerable to various routing attacks because it has an easy structure to attack such as packet eavesdropping or tapping by nature of the wireless environment and routing and data transmission are performed in a hop-by-hop manner by mobile nodes. 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 [19–22]. 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 [23–25]. 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 other is to deplete the energy of the attack node by including target nodes in many routes [26, 27].

The Jellyfish attack is an attack that interrupts data transmission by delaying transmission of data packet or discarding after the attack node normally transmits the RREQ or RREP packet for route discovery and the route through itself is set [28, 29]. 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. This leads to continuous attempts of message retransmission by nodes to recover the failed path and consumes a lot of energy on each node. As a result, in a wireless sensor network composed of sensor nodes with limited power, it is an important issue to apply a routing technique in which energy efficiently and effectively considers the defence against Jamming attacks [30].

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 [31]. 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. In this way, a secure route is set through a signature check on RREQ and RREP.

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 [32]. This technique creates a tree based on the base station and initializes the one-way hash chain. And, then, if the mobile node detects an event through its neighbor node, the data can be transmitted to the base station through the selected immediate node. Each node uses the only one-way hash chain that it manages in order to transmit securely data to the base station.

Feedback based secure routing protocol (FBSR) is an energy efficiency-oriented routing protocol using evaluation functions [33]. 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 [34]. The Ariadne technique is a DSR-based secure routing technique and uses authentication using MAC and shared keys. The source node creates the MAC value using a shared secret key in order to search route to the destination node and includes it in the RREQ. When the destination node receiving it authenticates the RREQ packet and transmits the RREP message, it is authenticated by the source node. Through this process, the source node can be set a secure route with the destination node [35–37].

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. Therefore, the structures of various trust-based security routing are discussed. Trust-based AODV routing protocol is a technique of isolating malicious nodes and is applied to the public key [38]. This has a disadvantage that route path discovery is delayed a lot because this does not allow intermediate nodes on the path to transmit RREP packets. The trust-embedded AODV (T-AODV) technique is an extension of the trust-based AODV technique in which the reliability is calculated by distributing and updated [39]. 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 in [39]. Each node monitors its neighbor and maintains its reliability directly. 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. Other nodes increase the opinion if a node behaves normally; otherwise, they decrease the opinion. The nodes authenticate each other by verifying the certificates of the nodes. This protocol cannot detect internal attacks that malicious nodes can refuse packet forwarding. 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 [40]. 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. TDSR technique has the advantage of not affecting the network life by using node selection and path discovery considering energy [41].

3. 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 agent node collects reliability of each neighbor node while supporting the trust management node. 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. For setting of security path between the source node and the destination node, the reliability of each node and the reliability average value of the cluster are reflected. And it detects anomaly nodes based on the traffic measurement on the set path. 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 nonrepudiation as a technique for providing a security function of a routing protocol without CA assistance. It is possible to perform the

more rapid authentication process and solve the certificate management problem because there is no certificate issuance process from the CA.

Figure 1 shows the system structure of the trust-based model secure routing technique proposed in this paper.

3.2. Reliability Measurement and Security Routing. In this paper, we use a hierarchical cluster structure for efficient trust evaluation and management of nodes. 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. The reliability measurement for nodes within each cluster is made on all nodes that act as trust agents. 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. Therefore, the quality of packet forwarding is reflected to improve the accuracy of reliability measurement. 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:

$$T(i) = \alpha \frac{F_i(p_j)}{G_i(p_i)} + \beta \frac{F_i(D_j)}{G_i(D_i)}. \quad (1)$$

Here, α and β mean the weight according to the time that node i and node j participate in the network. $G_i(p_j)$ means that node j delivers the generated packet to node i, $F_i(p_j)$ means that node j is packet delivered to node i packet received from the neighbor node. And $G_j(p_i)$ means that node i delivers to node j generated packet, $F_j(p_i)$ means that node i is the packet delivered to node j packet received from the neighbor node. This 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 security path between the source node and the destination node is set based on the reliability for each node calculated by the abovementioned method. The reliability information for all nodes participating in the network is stored in the trust information table (TIT) in the trust management node. Figure 2 shows the structure of the trust information table.

As shown in Figure 2, the reliability of node A is stored neighbor node transmitted packet from node A, and the value is calculated by node H and node S. The reliability value measured by each neighbor node is recalculated by the following equation:

$$T(K) = \text{avg}\left(\sum_{i=0}^{n} T_i(K)\right). \quad (2)$$

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 (3). Ci means the number of clusters constituting the network and is an expression for calculating the average reliability of each cluster:

$$C_i T(K) \frac{\sum_{i=0}^{n} N_i T(k)}{N+1}. \quad (3)$$

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. And then, the path with the highest reliability value is selected. Figure 3 shows an example of a reliability-based path setting. As shown in the figure, there are several paths from the source node (S) to the destination node (D). Among them, the node F, the node *J*, and the node *L* are excluded from the route setting because they are less than the reliability value of the cluster. Therefore, the security path based on the reliability is that the path having a higher average value of all paths than the path length is selected.

3.3. Security Data Transmission Technique. In the method mentioned in the previous section, the key exchange technique is applied for secure data transmission after the secure path is established between a source node and a destination node. 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 information is signed using the public key shared between trust management nodes to prevent falsification from nodes. This trust information is used as information to guarantee its identity for secure data transmission at the time of key exchange. 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. The source code generates a shared key and encrypts it to the public key of the destination node and

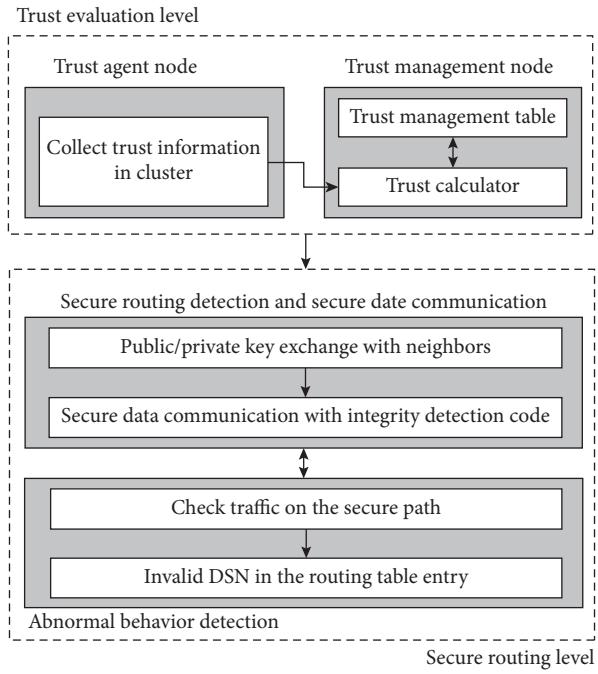

Figure 1: The trust-based model routing system structure.

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 the trust information table.

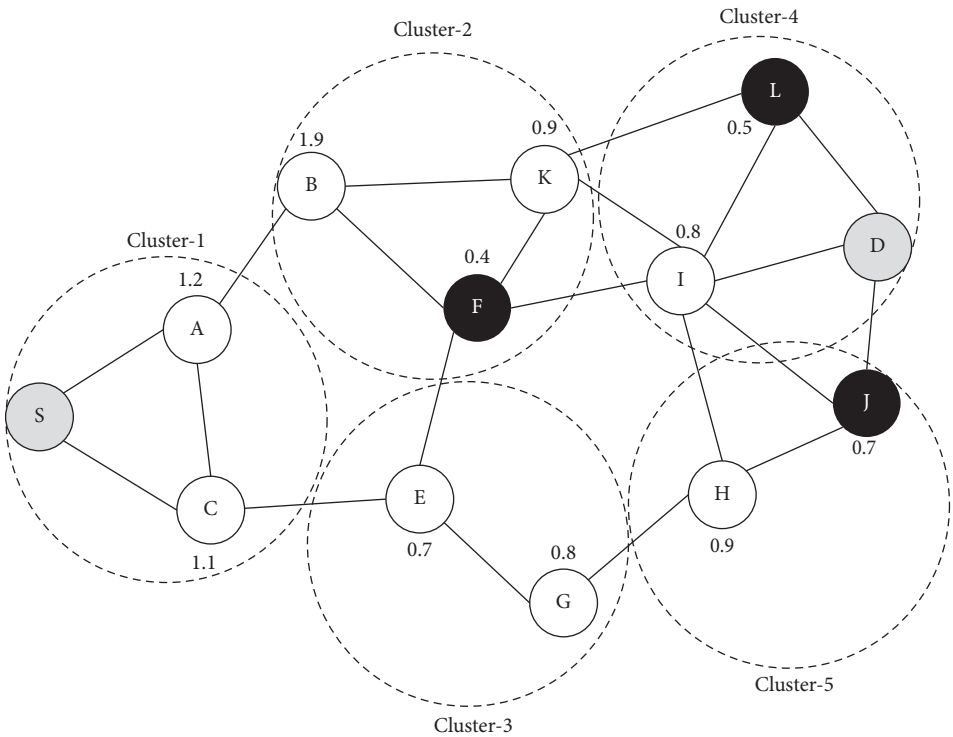

Figure 3: Path setting flow diagram based on trust values.

transmits. 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 process described above is shown in Figure 4. 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.

Key_Req means a key agreement request, S_(pub_key) means a public key of a source node, and IDC(hash(-S_(pub_key))) means an integrity check code for its public key. Key_Rep means a key agreement response, S_(sec_key) means a secret key of the source node, and IDC(hash(S_(sec_key))) means an integrity check code of its secret key.

3.4. Anomaly Detection. The performance of the routing protocol is reduced by malicious nodes in the network. In this section, the following process is performed in order to detect the anomaly nodes in the routing process. First, a suspicious node is detected in the secure path module through traffic checks on a node. Second, a malicious node is detected by a DSN check existing in a path table entry of the node. The traffic from the source node to the destination node will be measured for t hours. Here, t value uses the Round Trip Time (RTT) between the source node and the destination node, and the average value of the traffic is calculated by the following equation:

$$T = \frac{1}{\mathrm{RTT}\sqrt{(2B/3)p} + T_0 \min\left\{1, 3\sqrt{(3B/8)}\, p\right\} p\left(1 + 32p^2\right)}. \quad (4)$$

Here, T_0 represents the timeout and p represents the pack loss rate. If the value measured by equation (4) is higher than the average traffic of the cluster, it is judged that a malicious node exists in the path. And, it checks the DSN of the packets transmitted by nodes existing in the path and detects a wrong DSN. The false DSN check is an important factor for detecting anomaly node because it relies on the DSN to grantee loop-free to the destination node. Routing information checks are performed in preparation for an attack that may occur in the data transmission step. In this process, it detects an anomaly node that responds to non-existent node ID or transmits a packet using an invalid DSN. The information of the detected node is transmitted to the trust management node, the reliability value is set to 0, and the routing participation of the node is excluded. Figure 5 shows the anomaly detection process described above.

4. Experiments and Results

4.1. Simulation Parameters. In this section, we evaluate the main performance of the trust-based model secure routing technique proposed in this paper. The simulations are conducted in NS2. The experimental environment for simulation is as follows: 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. The type of Jamming attack used in this experiment used deceptive Jamming operating on the network layer. Table 3 shows the experimental variables used for the experiment.

4.2. Performance Metrics. We experimented in two ways in order to evaluate the performance of the proposed technique in this paper. 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

5. Results and Analysis

Figure 6 shows 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. Therefore, we confirmed that the performance was greatly degraded with the Hello flooding attack taking a normal action until the path setting. However, the proposed technique showed excellent performance in the Hello flooding attack because data transmission takes

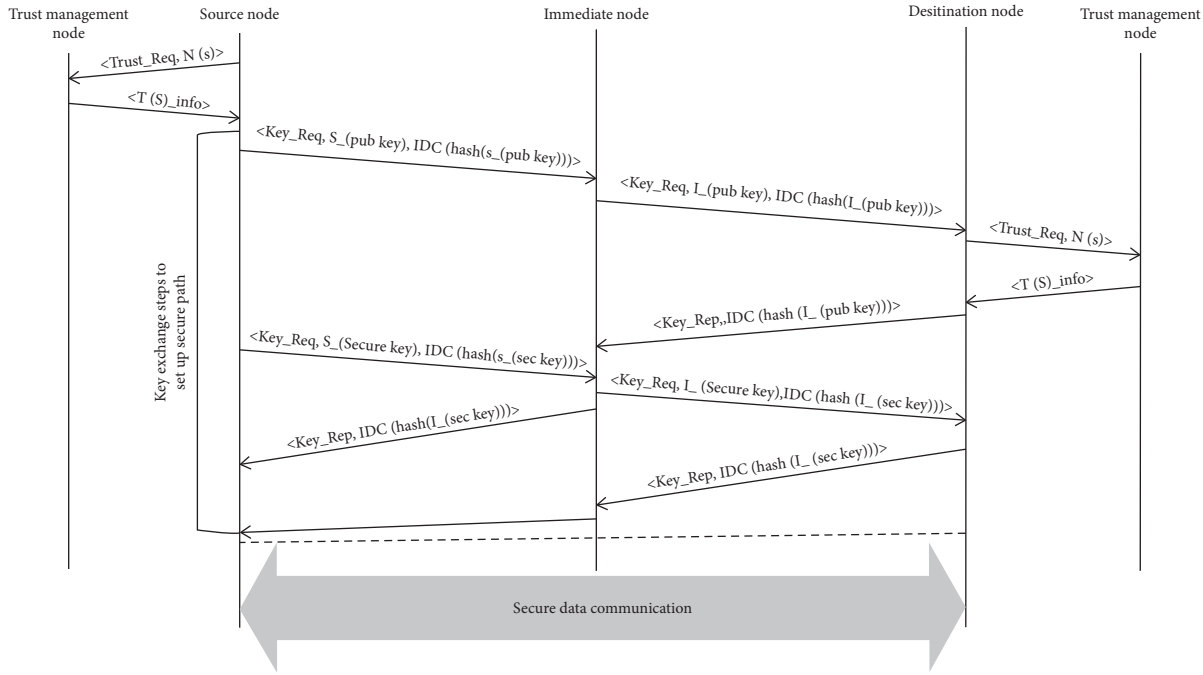

Figure 4: Internodes key exchange process for secure data communication.

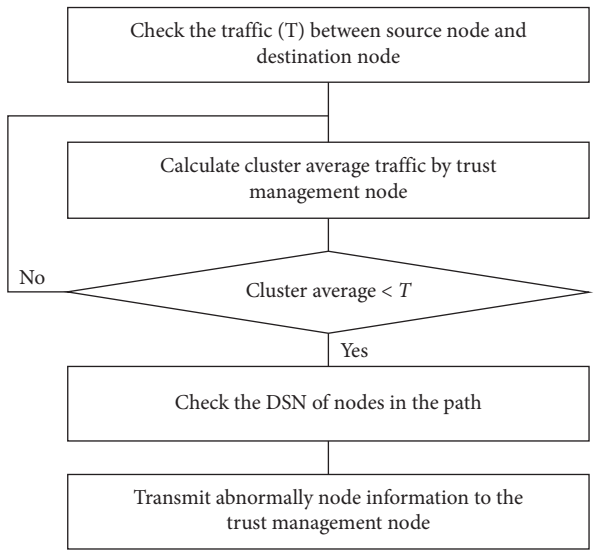

Figure 5: Anomaly node detection process with DSN examination on path.

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

place after performing the key exchange process with the source node and the destination node even after setting the path.

Figure 7 shows the result of measuring the packet transmission ratio according to the presence of a Jellyfish attack. As the results show, the performance of the SAODV was not good when the Jellyfish attack occurred. 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. However, the proposed technique showed the result of the excellent performance for the Jellyfish attack because it performs key exchange process between the source node and the destination node and data is transmitted even after routing.

Figure 8 shows the result of confirming the effect of packet delivery between the source node and the destination node due to the Jamming attack. 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 9 shows the measurement result of transmission delay time between the source node and the destination node by Hello flooding attack, Jellyfish attack, and Jamming attack. The SAODV technique uses TTL values and digital signatures of RREQ and RREP for secure routing. The delay

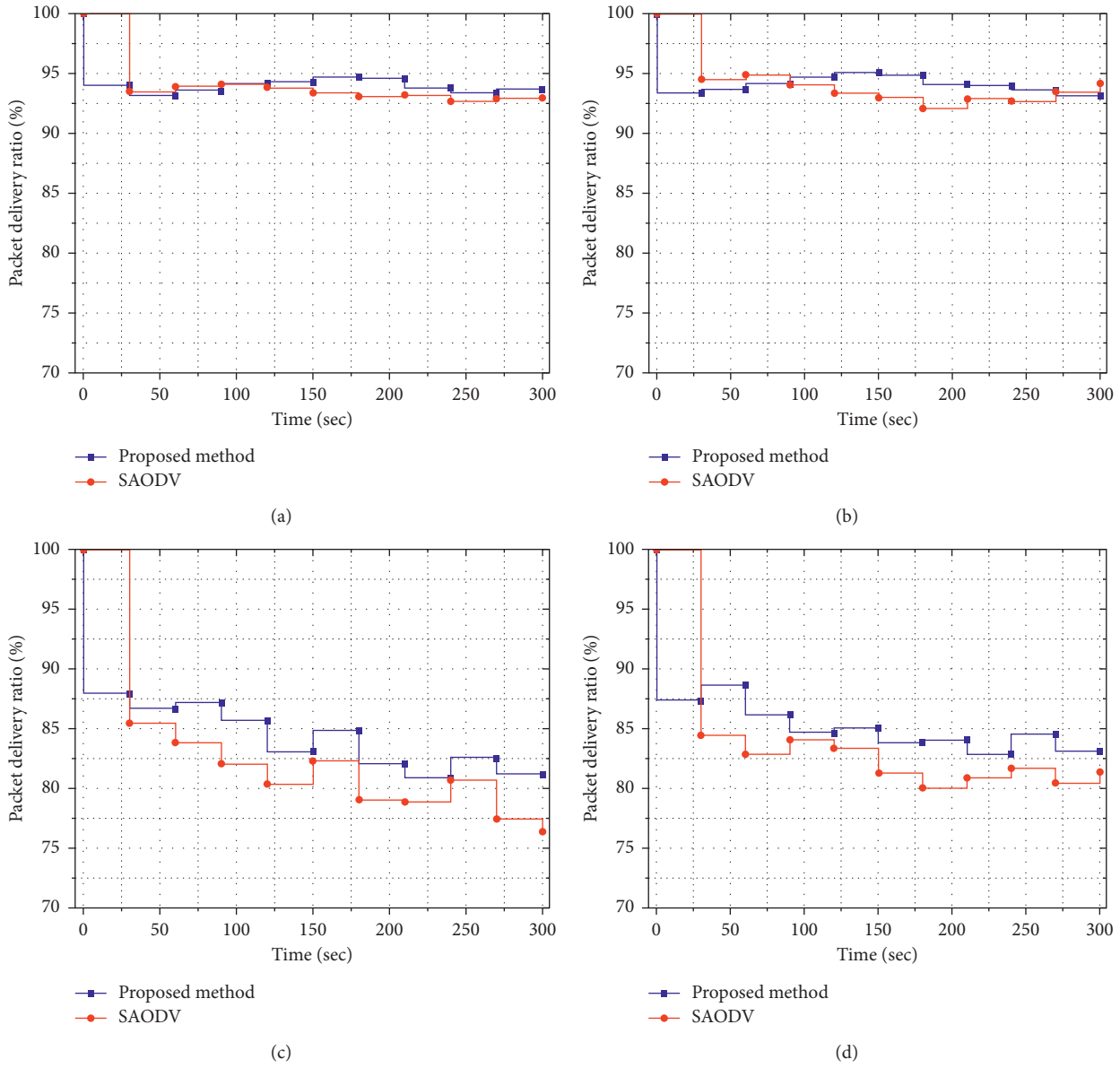

Figure 6: Results of packet delivery rates based on the presence of Hello flooding attacks (a) Measurement results of 50 nodes without Hello flooding attack. (b) Measurement results of 100 nodes without Hello flooding attack. (c) Measurement results of 50 nodes in Hello flooding attack. (d) Measurement results of 100 nodes Hello flooding attack.

time exists due to this authentication process, and it is longer when an attack occurs. In particular, it is also the cause of low-security performance for attacks after setting the path. We confirmed that the proposed technique was not significantly affected by the attack, but the end-to-end latency appeared rather long because data is transmitted after the path setting based on the reliability of the nodes and key exchange process between the source node and the destination node.

The number of control packets can influence the overall performance of the network. Figure 10 shows the measurement result of the number of control packets generated in each technique during the experiment time. The SAODV technique showed the authentication process for secure path set, and the number of control packets increases. Also, the more nodes moved, the more the amount increased. The proposed technique showed stable performance with little change in the number of control packets even in the event of an attack although it does not go through the authentication server and the control packet is rather high by key exchange between nodes for secure data transmission.

Figure 11 shows the result of the network throughput depending on the existence of Jellyfish attack. The network throughput is an important indicator which can confirm the performance of the routing protocol as the amount of data transmitted from the source node to the destination node during the unit time. SAODV showed a large difference

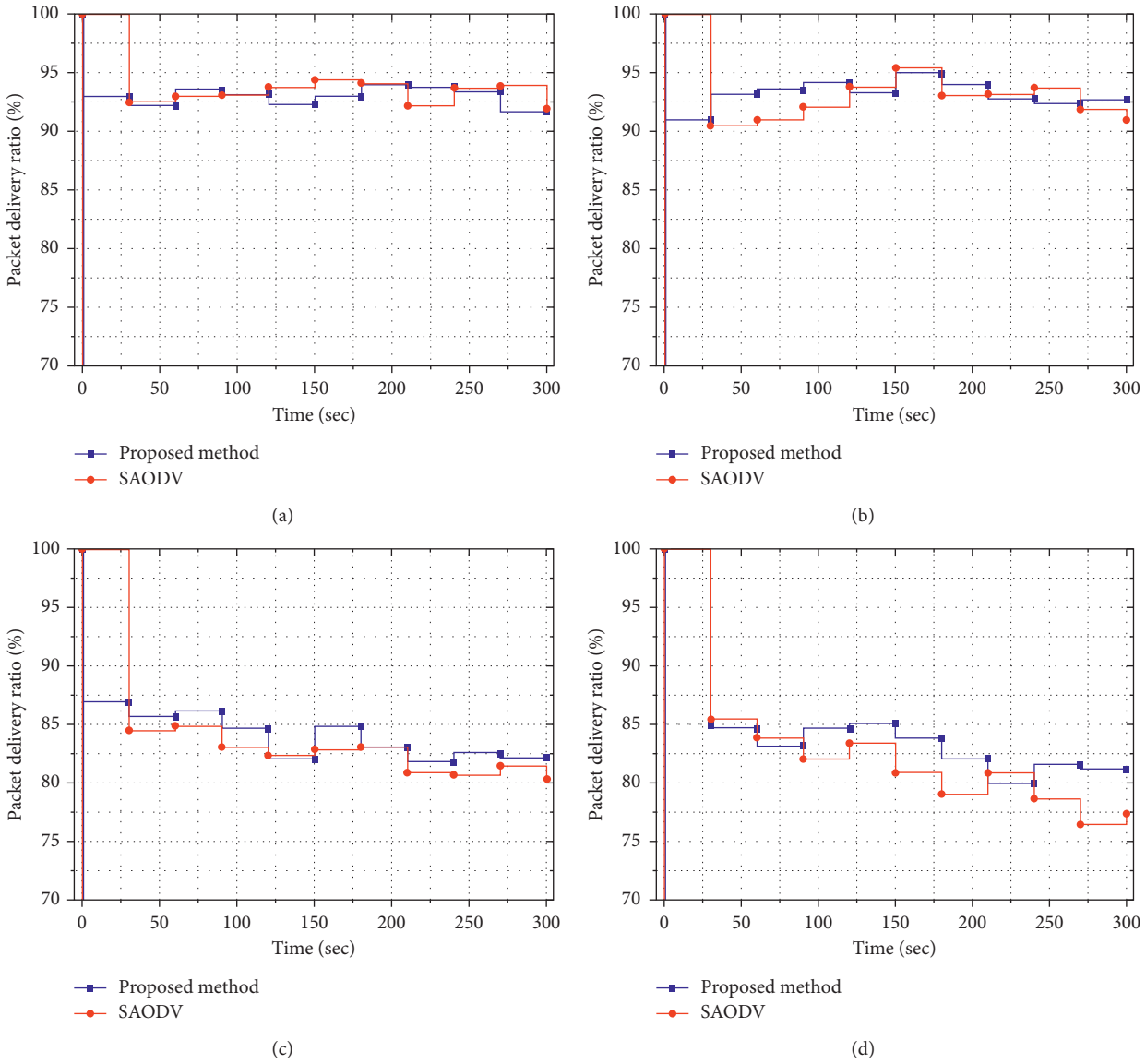

Figure 7: Results of packet delivery rates based on the presence of Jellyfish attacks. (a) Measurement results of 50 nodes without the Jellyfish attack. (b) Measurement results of 100 nodes without the Jellyfish attack. (c) Measurement results of 50 nodes in the Jellyfish attack. (d) Measurement results of 100 nodes in the Jellyfish attack.

depending on the existence of Jellyfish attack because the security technique is not applied during data transmission. But the proposed technique applies the average reliability of the cluster and the reliability of the nodes existing in the path during the path setting and goes through an anomaly detection process based on the traffic. Therefore, the technique is not influenced by the presence of Jellyfish and shows superior performance compared to SAODV.

Figure 12 shows the measurement result of the average path length between the source node and the destination node according to the movement time of nodes and the attack. The average path length becomes longer as the movement speed of nodes is faster. The proposed technique shows the long path length because it sets the path with higher reliability than the path length. It shows that the path length depending on the attack is also long and the proposed technique is less influenced by the attack due to secure data communication through key exchange and traffic-based malicious node detection process.

The routing overhead describes the number of routing packets for route discovery and route maintenance needed to be sent in order to propagate the CBR packets. Figure 13 shows the comparison result of routing overhead between SAODV and the proposed technique. As the number of malicious nodes increases, routing overhead also increases. SAODV is not significantly affected by attacks because it authenticates control packets in the route discovery step. Routing overhead is increased greatly as it is vulnerable to

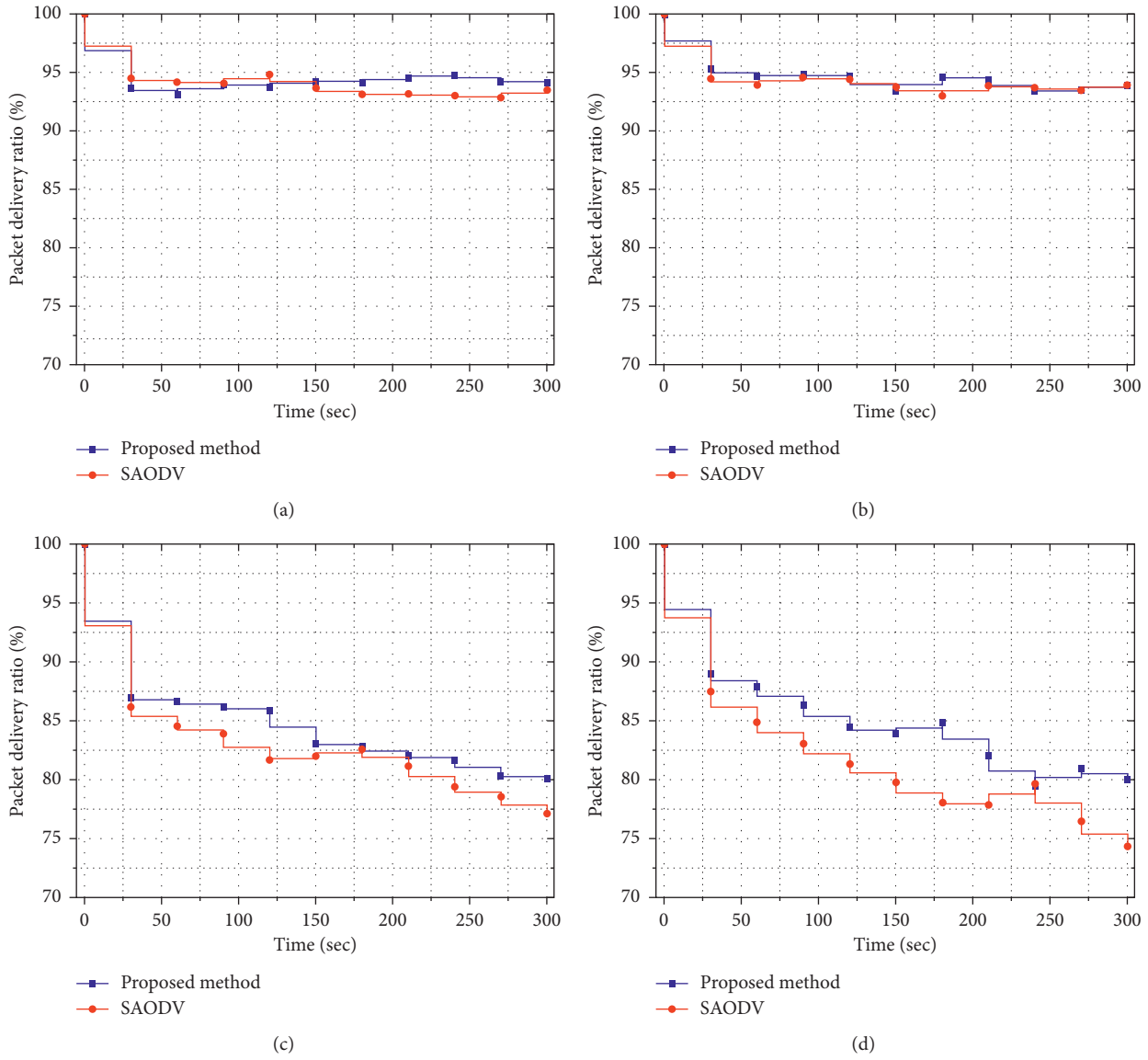

Figure 8: Results of packet delivery rates based on the presence of Jamming attacks. (a) Measurement results of 50 nodes without Jamming attack. (b) Measurement results of 100 nodes without Jamming attack. (c) Measurement results of 50 nodes in Jamming attack. (d) Measurement results of 100 nodes in Jamming attack.

attacks in the data transmission process. 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 14 shows the experimental results for EAODV and the packet transmission rate when the number of nodes is 50 and 100 to evaluate the routing performance. 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.

In Figure 15, the throughput which is an important metric shows the result depending on the number of nodes and the moving speed. We can see that the network throughput gradually decreases as the moving speed of the node increases. This means that as link failures by the movement of the nodes increase and the demand for new routing increases, the consumption of bandwidth increases. As the result shows, the proposed technique that the node is managed by the cluster head shows better performance than EAODV.

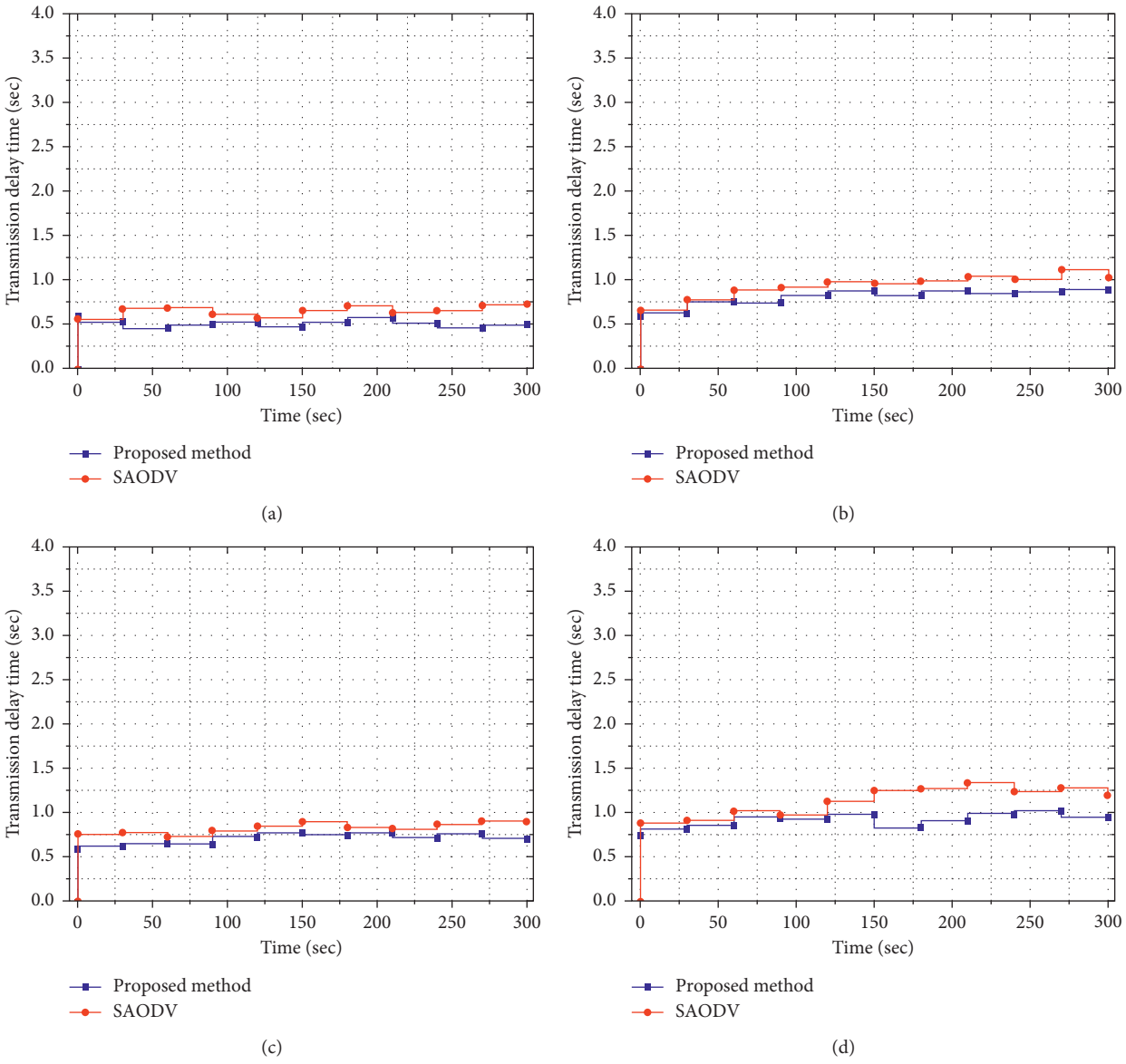

Figure 9: Results of transmission delay time due to Hello flooding attack, Jellyfish attack, and Jamming attack. (a) Measurement results of 50 nodes without attacks. (b) Measurement results of 50 nodes in Hello flooding attack. (c) Measurement results of 50 nodes in Jellyfish attack. (d) Measurement results of 50 nodes in Jamming attack.

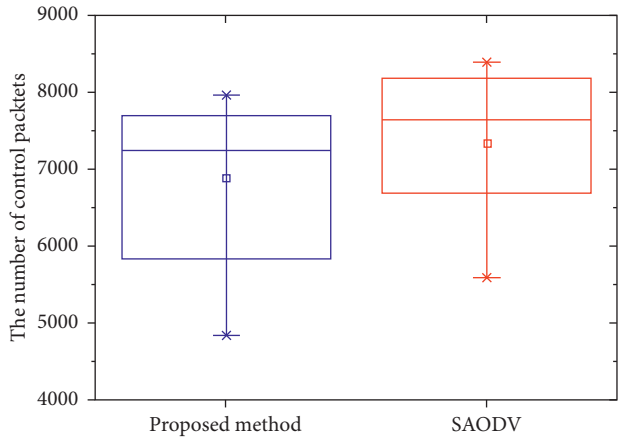

Figure 10: Amount of control packets.

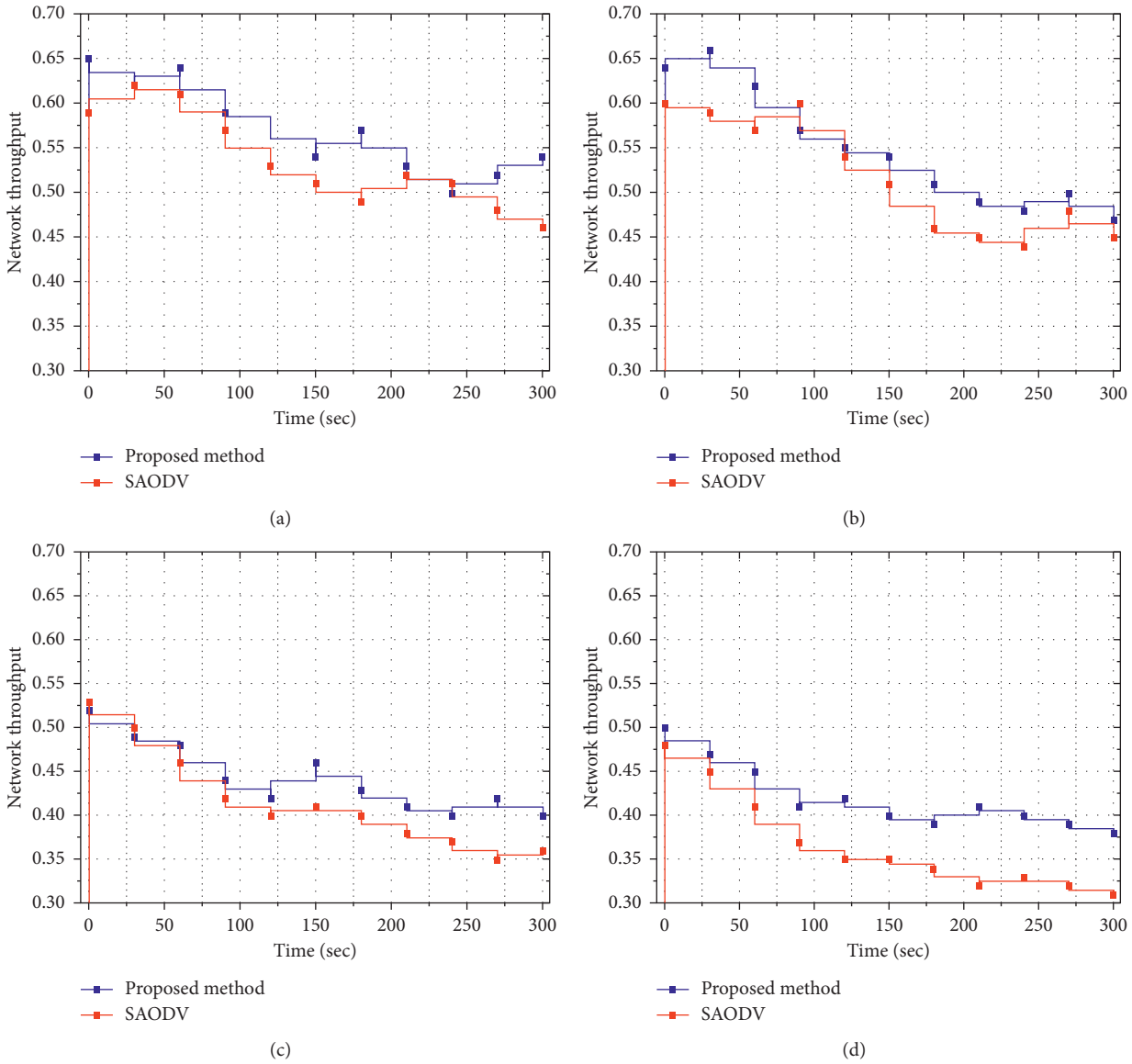

Figure 11: Results of network throughput based on the presence of Jellyfish attacks. (a) Measurement results of 50 nodes without Jellyfish attack. (b) Measurement results of 100 nodes without Jellyfish attack. (c) Measurement results of 50 nodes in Jellyfish attack. (d) Measurement results of 100 nodes in Jellyfish attack.

The comparison between the number of routing packets and the node speed is shown in Figure 16. 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.

6. 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. In order to improve the accuracy of reliability, the quality of the packet as well as the number of packets transmitted between the nodes was included. That is to reflect in the reliability calculation by determining whether a packet received from a neighbor node is generated. 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

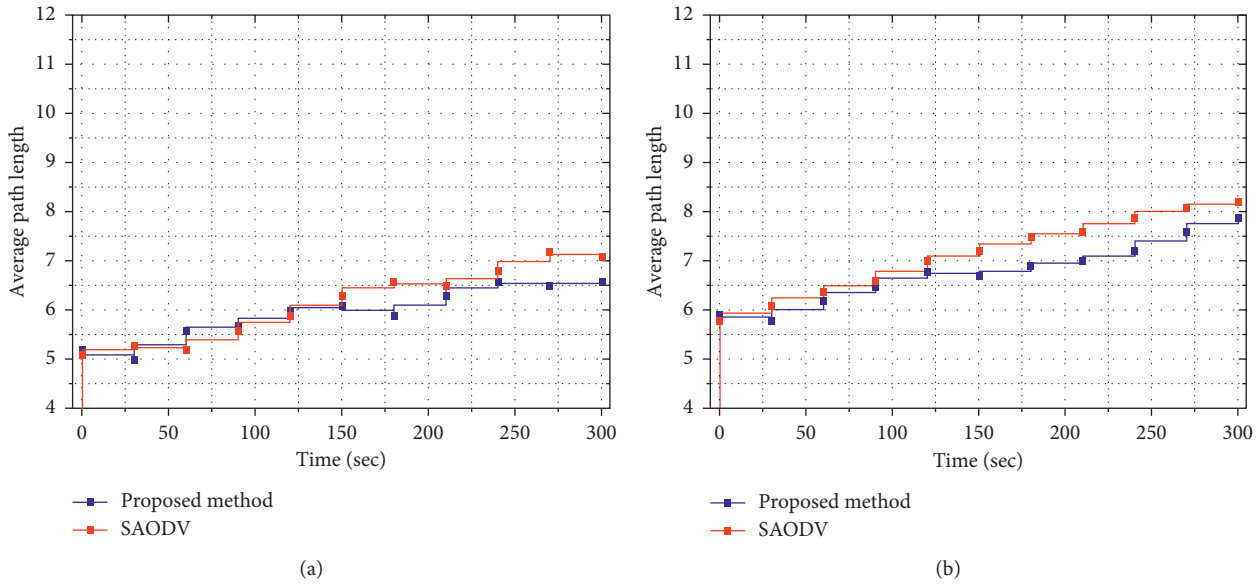

Figure 12: Results of the average path length due to Hello flooding attack. (a) Measurement results of 50 nodes without Hello flooding attack. (b) Measurement results of 50 nodes in Hello flooding attack.

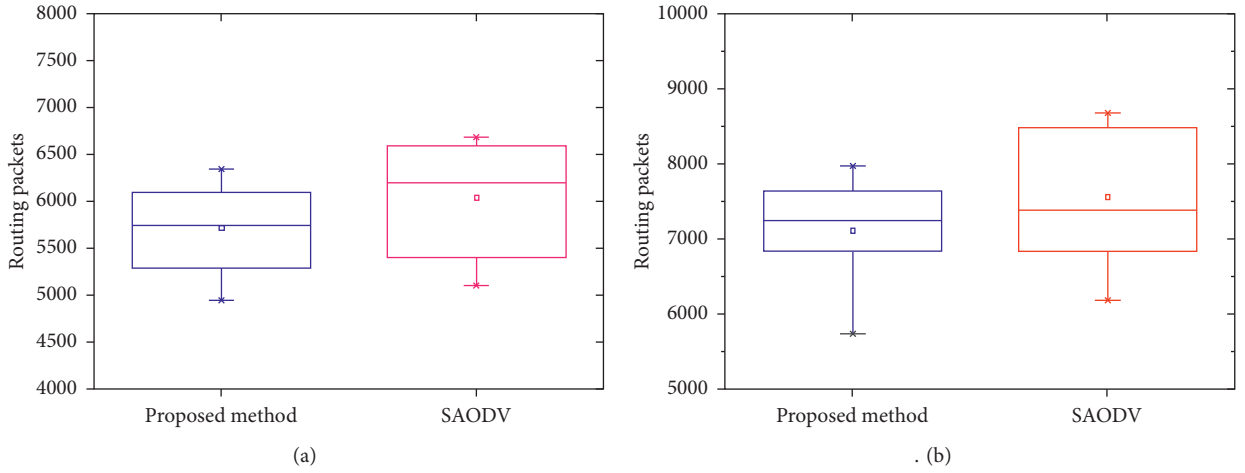

Figure 13: Routing overhead depending on the number of nodes. (a) Measurement results of 50 nodes. (b) Measurement results of 50 nodes.

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. The path setting was made by combining the reliability of the measured nodes and the reliability average value of each cluster. 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. The path with the highest reliability among the remaining nodes was selected. 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. If the traffic occurring from a specific path was higher than the average traffic in the cluster, the nodes in the path checked the DSN of the transmitted packet, the node transmitted the

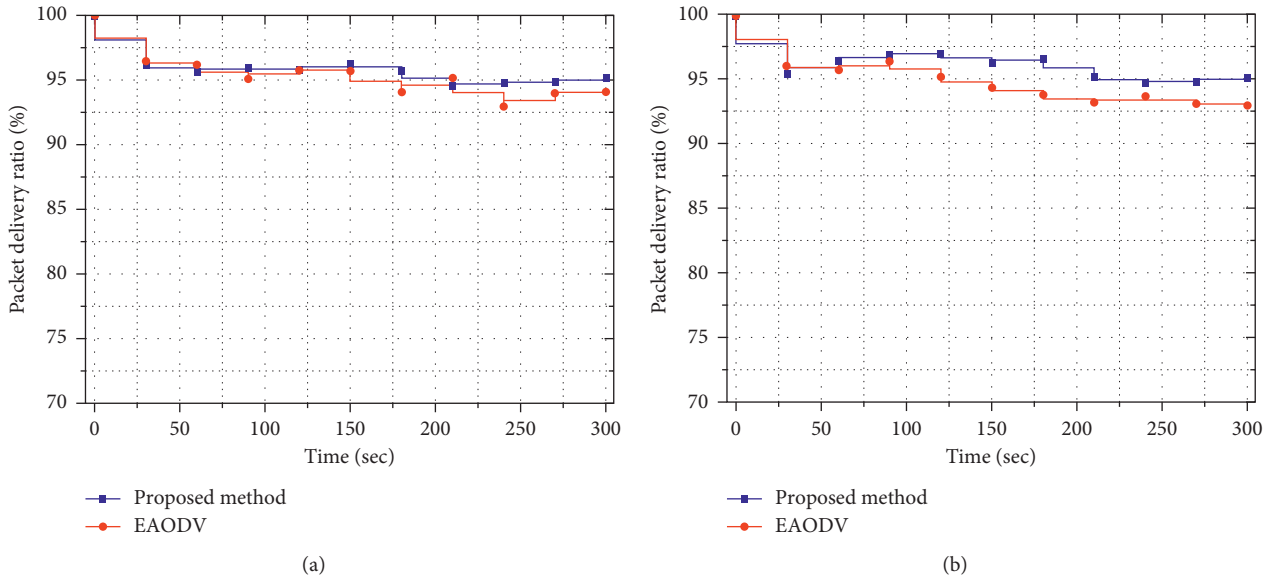

FIGURE 14: Routing overhead depending on the number of nodes. (a) Measurement results of 50 nodes without Hello flooding attack. (b) Measurement results of 50 nodes in Hello flooding attack.

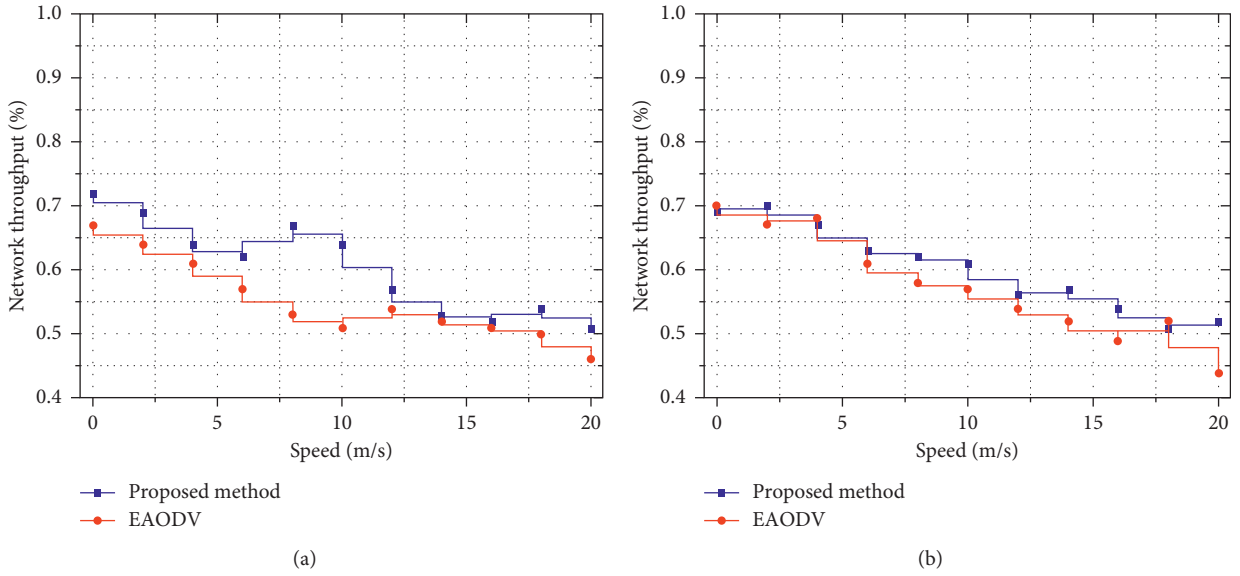

FIGURE 15: Network throughput depending on the number of nodes. (a) Measurement results of 50 nodes. (b) Measurement results of 100 nodes.

wrong DSN was recognized, and network participation was excluded. 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. In addition, to evaluate the routing performance, the experiments are performed on packet transmission rate, throughput, and routing packet performance criteria with EAODV. 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

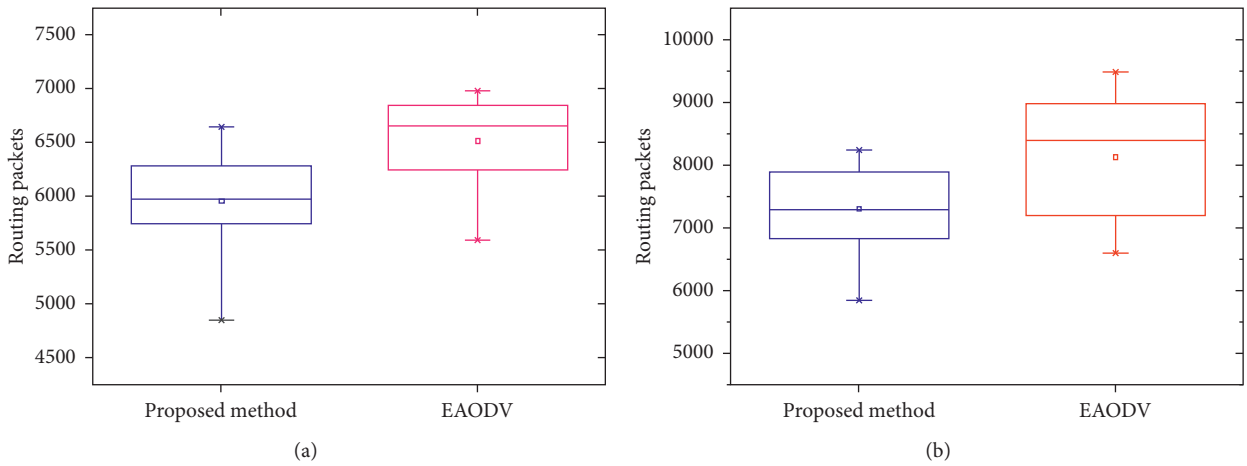

Figure 16: Routing overhead depending on the number of nodes. (a) Measurement results of 50 nodes without Hello flooding attack. (b) Measurement results of 50 nodes in Hello flooding attack.

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. In the future, research on the energy-aware trust model will be conducted to improve the efficiency of the secure routing protocol.

Data Availability

The simulated evaluation data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper was supported by Joongbu University Research & Development Fund, in 2019.

References

[1] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 70–75, 2002.

[2] M. Gunes, U. Sorges, and I. Bouazizi, "ARA-the ant-colony based routing algorithm for MANETs," in *Proceedings of the International Conference on Parallel Processing Workshop*, Vancouver, BC, Canada, August 2002.

[3] C. Mbarushimana and A. Shahrabi, "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, May 2007.

[4] S. Mittal and P. Kaur, "Performance comparison of AODV, DSR and ZRP routing protocols in MANET's," in *Proceedings of the International Conference on Advances in Computing, Control, and Telecommunication Technologies*, Trivandrum, India, December 2009.

[5] S. Seys and B. Preneel, "ARM: Anonymous routing protocol for mobile ad hoc networks," in *Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06)*, Vienna, Austria, April 2006.

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

[7] M. A. Mikki, "Energy efficient location aided routing protocol for wireless MANETs," 2009, http://arxiv.org/abs/0909.0093.

[8] B. Divecha, "Impact of node mobility on MANET routing protocols models," *JDIM*, vol. 5, no. 1, pp. 19–23, 2007.

[9] P. Gupta, P. Goel, P. Varshney, and N. Tyagi, "Reliability factor based AODV protocol: Prevention of black hole attack in MANET," in *Smart Innovations in Communication and Computational Sciences*, pp. 271–279, Springer, Berlin, Germany, 2019.

[10] M. A. Mahdi, T.-C. Wan, and R. Abdullah, "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, April 2019.

[11] A. Mandhare and S. Kadam, "Performance analysis of trust-based routing protocol for MANET," in *Computing, Communication and Signal Processing*, pp. 389–397, Springer, Berlin, Germany, 2019.

[12] M. Medadian, M. H. Yektaie, and A. M. Rahmani, "Combat with black hole attack in AODV routing protocol in MANET," in *Proceedings of the First Asian Himalayas International Conference on Internet*, Kathmundu, Nepal, November 2009.

[13] N. A. M. Saudi, M. A. Arshad, A. G. Buja, A. Firdaus, A. Fadzil, and R. M. d. Saidi, "Mobile ad-hoc network (MANET) routing protocols: A performance assessment," in *Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017)*, Langkawi, Malaysia, June 2019.

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

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

[16] D. Wadbude and V. Richariya, "An efficient secure AODV routing protocol in MANET," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 1, no. 4, pp. 274–279, 2012.

[17] P. Nayak, R. Agarwal, and S. Verma, "Energy aware AODV (EA-AODV) using variable range transmission," *Advances in Computer Science, Engineering & Applications*, pp. 589–597, 2012.

[18] J. Tian, Y. Wang, and J. Lv, "Researching on AODV and PS-AODV routing protocols of ad hoc network for streaming media," in *Proceedings of the International Conference on Computer Application and System Modeling*, Taiyuan, China, July 2012.

[19] A. Chandra and S. Thakur, "Qualitative analysis of hybrid routing protocols against network layer attacks in MANET," in *Proceedings of the International Journal of Computer Science and Mobile Computing*, vol. 4, no. 6, pp. 538–543, 2015.

[20] H. Moudni, M. Er-rouidi, H. Mouncif, and B. El Hadadi, "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, February 2016.

[21] R. L. Rao, B. Satyanarayana, and B. Kondaiah, "Performance of CBIDS on AODV routing protocol against black hole attacks in MANET," 2018.

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

[23] A. K. Jain and V. Tokekar, "Mitigating the effects of black hole attacks on AODV routing protocol in mobile Ad Hoc networks," in *Proceedings of the International Conference on Pervasive Computing (ICPC)*, Pune India, January 2015.

[24] S. Singh, A. Mishra, and U. Singh, "Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm," in *Proceedings of the Symposium on Colossal Data Analysis and Networking (CDAN)*, Indore, Madhya Pradesh, India, March 2016.

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

[26] B. Sen, M. Goldie Meitei, K. Sharma, M. Kanti Ghose, and S. Sinha, "A trust-based intrusion detection system for mitigating blackhole attacks in MANET," in *Advanced Computational and Communication Paradigms*, pp. 765–775, Springer, Berlin, Germany, 2018.

[27] S. Tan, X. Li, and Q. Dong, "Trust based routing mechanism for securing OSLR-based MANET," *Ad Hoc Networks*, vol. 30, pp. 84–98, 2015.

[28] F. Ahmed, S. Rashid, and M. Rahman, *Impact of Black-Hole and Jellyfish Attacks in MANET Using HTTP Traffic*, BRAC University, Dhaka, Bangladesh, 2016.

[29] A. K. Ali, B. Sharma, and U. M. Sharma, *Impact analysis of JellyFish attack in MANETs*, ADBU Journal of Engineering Technology, Guwahati, Assam, India, 2016.

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

[31] M. A. Abdelshafy and P. J. B. King, "AODV and SAODV under attack: Performance comparison," in *Proceedings of the International Conference on Ad-Hoc Networks and Wireless*, Benidorm, Spain, June 2014.

[32] A. K. Das, R. Chaki, and K. N. Dey, "Secure energy efficient routing protocol for wireless sensor network," *Foundations of Computing and Decision Sciences*, vol. 41, no. 1, pp. 3–27, 2016.

[33] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou, "FBSR: Feedback-based secure routing protocol for wireless sensor networks," *International Journal of Pervasive Computing and Communications*, vol. 4, no. 1, pp. 61–76, 2008.

[34] H. Zhao, "A new secure geographical routing protocol based on location pairwise keys in wireless sensor networks," *International Journal of Computer Science Issues (IJCSI)*, vol. 10, no. 2, p. 365, 2013.

[35] G. Padmavathi, P. Subashini, and D. D. Aruna, "CCMP-AES model with DSR routing protocol to secure link layer and network layer in mobile adhoc networks," *International Journal on Computer Science and Engineering*, vol. 2, no. 5, 2010.

[36] I. Woungang, S. K. Dhurandher, M. S. Obaidat GE, and R. D. Peddi, "A DSR-based routing protocol for mitigating blackhole attacks on mobile ad hoc networks," *Security and Communication Networks*, vol. 9, no. 5, pp. 420–428, 2016.

[37] I. Woungang, "Detecting blackhole attacks on DSR-based mobile Ad Hoc networks," in *Proceedings of the International Conference on Computer, Information and Telecommunication Systems (CITS)*, Amman, Jordan, 2012.

[38] P. Samundiswary and P. Dananjayan, "Performance analysis of trust based AODV for wireless sensor networks," *International Journal of Computer Applications*, vol. 4, no. 12, pp. 6–13, 2010.

[39] D. Kukreja, U. Singh, and B. Reddy, "A survey of trust based routing protocols in MANETs," *Journal of Advances in Computer Networks*, vol. 1, no. 4, pp. 280–285, 2013.

[40] Y. Ren, Z. Zheng, T. Wang, and S. Zhang, "A Trust-based minimum cost and quality aware data collection scheme in P2P network," *Peer-To-Peer Networking and Applications*, pp. 1–24, 2020.

[41] Y. Liu, X. Liu, A. Liu, N. N. Xiong, and F. Liu, "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, 2019.