I. J. Computer Network and Information Security, 2022, 2, 1-13
Published Online April 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2022.02.01

A Study on Performance Improvement of Intrusion Detection using Efficient Authentication and Distributed Monitoring

Hwanseok Yang
Dept. of Information Security Engineering, Joongbu University, Goyang, 10279, Republic of Korea
E-mail: yanghs@joongbu.ac.kr

Received: 13 August 2021; Revised: 24 September 2021; Accepted: 21 November 2021; Published: 08 April 2022

Abstract: In a Mobile Ad hoc Network (MANET), mobile nodes play multiple roles as hosts and routers and are dynamically changing multi-hop structures. MANET consists only of wireless nodes with limit processing power, and routing and data transfer are performed through cooperation with each other. It is exposed to many attack threats due to the dynamic topology by the movement of the nodes and the characteristic of multi-hop communication. Therefore, in MANET, a technique that can detect effectively must be applied while detecting malicious nodes and reducing the impact of various attacks. In this paper, we propose a trust based authentication technique for nodes and a distributed monitoring technique to improve the detection performance of malicious nodes. The hierarchical cluster structure was used to improve authentication of nodes and detection performance and management efficiency of malicious nodes. A lightweight authentication technique of member nodes in the cluster was applied and the efficiency of node authentication was improved. It was used to determine whether it was an attack node by transmitting traffic monitoring information for neighbor nodes to CA and using. In addition, the efficient authentication technique using only key exchange without anyone's help was applied in order to provide integrity when exchanging information between cluster heads. Through this, it was possible to be free from trust information about nodes and forgery and falsification of information about attack nodes. The superiority of the technique proposed in this paper was confirmed through comparative experiments with the existing intrusion detection technique.

Index Terms: Authentication Technique, Intrusion Detection System (IDS), Distributed Monitoring, Mobile Ad-Hoc Network (MANET).

1. Introduction

The wireless network is largely divided into a network formed based on a fixed infrastructure and a Mobile Ad-hoc Network (MANET) formed only by wireless nodes without the help of the infrastructure. That is, MANET is a network configured by freely cooperating among wireless nodes without the help of a fixed base. In MANET, the network topology is constantly changing because of the frequent movement of wireless nodes and there are many restrictions on resources. Therefore, MANET requires protocols that use network resources efficiently. In particular, the routing protocol is an important protocol that influences performance in a MANET environment with multi-hop communication. However, the routing protocol applied in the existing network cannot be applied as it is. And it is easily exposed to many security threats due to the dynamic environment by the movement of nodes and the characteristics of the wireless environment. Many security routing techniques have been studied to prevent such routing attacks [1,2,3]. These studies are largely divided into a technique for collecting network-wide information, an authentication technique for nodes participating in the network, and a geographical routing technique. Nevertheless, there are many types of attacks in MANET because of many characteristics that are vulnerable to security. Therefore, an authentication technique through accurate trust evaluation of nodes participating in the network is very important [4,5]. The intrusion detection technique which is efficient for malicious nodes and minimizes the impact from these attacks is essential. This technique must have the ability to detect multiple attacks at the same time while reducing the false positive rate. As a result, network life and reliability will be increased.

In the study on intrusion detection using distributed monitoring, the false detection rate was high because reliability evaluation of the nodes constituting the cluster was not performed [6]. In order to solve these shortcomings, trust evaluation of nodes and the cluster key issuance technique are applied in this paper. In this paper, we propose an authentication method through efficient trust evaluation of nodes and a distributed monitoring method for efficient detection of specific attacks in dynamic environment. The hierarchical cluster is applied for the proposed technique. The node with the highest connectivity in the cluster is selected as the Certification Authority (CA), and the CA node plays

the role of administrator in monitoring for authentication and intrusion detection. The node authentication method consists of a combination of local trust information and global trust information, and the CA stores trust information in Member Trust Table (MTT). For distributed monitoring, all nodes participating in the network monitor traffic to neighboring nodes within 1-hop distance and measure the packet forwarding rate, packet generation rate, and packet discard rate. Measured parameter values are stored as multidimensional vector, and CA detect attack nodes by using these values. In addition, in order to provide integrity when exchanging attack node information and trust information of nodes between CAs, an authentication method is applied only through the public key and shared key exchange process without the help of any CA. In this way, it is possible to ensure fast and secure data transmission of nodes. Through the proposed technique, it is possible to accurately evaluate the trust of nodes participating in the network and to effectively exclude malicious nodes from participating in the network. The structure of this paper is as follows. In chapter 2, the routing protocol, security routing technique, and intrusion detection technique applied in MANET is described. In chapter 3, the security technique for reliability improvement proposed in this paper is explained. In chapter 4, the performance of the proposed method is evaluated through experiments and finally, chapter 5 concludes.

2. Related Research

2.1. Routing Protocols

Routing protocol in MANET can be classified into a table management method using Bellman-Ford algorithm used in a wired environment, the on-demand method considering the environment of MANET, and a hybrid method that combines the advantages of these two methods.

In the table management method, each node stores the whole route of all nodes in the network into each entry of table. So, the latest network information is always maintained by broadcasting routing information when the network topology changes. It has the advantage of quick connection setup because it has the route information when there is a connection request by traffic generation. But the broadcasting overhead of the control message for route management is too large and the resource is wasteful for route discovery that is not used for frequent phase change. Although this method is suitable for a small ad hoc network with a small number of nodes, it has many disadvantages in medium and large networks [7].

There is Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Cluster head Gateway Switching Routing (CGSR), Source-Tree Adaptive Routing (STAR) in this routing protocol [8,9,10].

In the On-demand method, the shortcomings of the table management method are solved. It does not always maintain the whole route for all mobile nodes in the network and performs the route acquisition process only when data transmission is required because it is a protocol proposed to be suitable for the MANET environment [11]. So, when the connection is requested, there is broadcasting overhead for setting a path to the destination node. Because of this, it has the advantage of increasing the delay time for the route discovery. But it has the advantage of being able to set a route. This method is focused on minimizing the delay time of route search as well as optimal route search because the initial route search is delayed in the routing protocol of request-based method. Currently, it is known as the most suitable method for MANET, where nodes move frequently, and this routing protocols includes Dynamic Source Routing (DSR), Ad-hoc On-demand Distance Vector (AODV), Associativity-Based Routing (ABR), and Temporally-Ordered Routing Algorithm (TORA) [12,13,14,15]. Table 1 show the characteristics of on-demand routing protocols.

Table 1. The characteristics of on-demand routing protocol

	Advantage	Disadvantage
AODV	No route included in data packet Multicast support	The problem of periodic Hello message
DSR	Asymmetric link support Having multiple routes	Source routing overhead Wrong cache problem
ABR	Partial rerouting of intermediate node Selection of long-lasting route	Periodic beacon issues
TORA	Having multiple routes Multicast support	Synchronization issues on all nodes

2.2. The secure routing technique

The Enhanced Average Encounter Rate-AODV (EAER-AODV) technique is a trust-based routing protocol based on opinions of nodes. In this technique, the opinions of nodes represent trust between nodes that are frequently updated according to the protocol specification. This technique selects a routing path according to the trust value of the neighbor node [16].

The Secure Routing-Based AODV technique proposed an approach method that detects an attacker node using a dynamic threshold to detect in order to detect a black hole attack and avoids full paths with attacker nodes [17]. Identification of the attacker node is performed during path formation.

Trust based Clustering and Secure Authentication (TCSA) technique is applied secure clustering and source node

authentication [18]. This technique is used the encryption key generated by source node in order to increase reliability, and all member nodes and the source nodes use the same route. And the identity of the node is checked by the agent node when a new node enters the cluster. In addition, the agent node also plays a role in monitoring the encrypted data if the data is tempered by the attack node.

Security-aware Adaptive DSR (SADSR) technique is one of the secure on-demand routing protocols, and every node has a route table with other nodes [19]. SADSR authenticates routing protocol message using digital signatures based on asymmetric cryptography. This manages multiple routes to a destination node and stores local reliability values for each node in the network. In order to set a route for multicast data transmission, the trust of all nodes on the route is calculated first, and data is transmitted using the route with the highest trust. By doing this, the trust of the data is increased and secure routing is provided.

Curve Based Secure Routing (CBSR) is a technique applied data encryption to the existing Curve Based Greedy Routing (CBGR) [20]. A route is set through a five-step process. First, mobile nodes encrypt their location information to neighboring nodes using a group key and transmit. And, in the base station, its location and necessary information encrypts to the destination node using one of the key chains and transmits. The encryption key is broadcasted by encrypting to the global key in order to set the route. Through this process, a routing route is formed and the set route is multiplex at this time. The goal node receives packets from multiple routes, compares the contents, and determines whether there is any change.

Secure Efficient distance vector routing in mobile wireless ad hoc networks (SEAD) technique includes sequence number in table update element to avoid routing loop problem of Destination Sequenced Distance Vector (DSDV) protocol [21]. This technique is a method of authenticating the sender on the receiving side of routing information. After the node requesting the route forms a hash chain, the hash value is included in update information of the routing table transmitted. The authentication procedures for neighbor nodes can use TELSA, TIK, etc., there is a disadvantage that a delay and overhead occur during authentication.

2.3. Intrusion detection technique

MANET is exposed to many attacks due to multi-hop data communication and dynamic topology. In MANET, security requirements such as availability, confidentiality, integrity, non-repudiation, and authentication must keep because these security vulnerabilities can cause serious problems. In particular, various intrusion detection techniques have been studied in preparation for many attacks that may occur in routing process. The characteristics of some techniques are as follows.

Dynamic Learning Method (DLM) is an attack detection technique based on dynamic learning [22]. The monitoring target for attack detection of this technique is the amount and the sequence number of RREQ and RREP. This monitors whether the threshold value judged to attack is exceeded. If it exceeds, it is regarded as an attack node. Otherwise, the last measured data is dynamically updated as a normal node.

Secure Routing Protocol (SRP) is a technique for detecting attacks by comparing the number of packets received from the source node and the number of packets sent [23]. That is, if there are more packets transmitted than received packets, the source node recognizes that an attack node using its ID exists and broadcasts a warning message. The disadvantage of this technique is that it is difficult to detect attacks on neighboring nodes except nodes existing in the route because attack detection through ACK is performed only between nodes communication with each other.

Prevention of a Co-operative Black Hole Attack (PCBHA) technique selects the node with the highest trust among the nodes that responded to the RREQ when the route is discovered and performs data transmission [24]. When the source node receives the ACK message from destination node, the reliability of neighboring nodes participating in data transmission is increased by 1, otherwise it is decreased by 1. In this way, a black hole attack is detected in the route.

Mobile Agent-IDS (MA-IDS) collects information about nodes within a certain range using a mobile agent [25]. Attack detection is performed by the attack detection algorithm being in the mobile agent. Although this technique has the advantage of reducing energy and network overhead, it has a disadvantage that it is difficult to apply if the transmission range in a large network is narrow.

In [26], techniques that provide important and low-cost technology through IDS design using artificial intelligence among the new techniques for intrusion detection were presented. By applying artificial neural network (ANN) to intrusion detection technique, it can help to eliminate the weakness of rule-based IDS. ANN-based IDS can be more effectively if properly trained on both normal and abnormal data sets. Therefore, it can be said that data set is important in this technique. Genetic algorithm is a widely used technique in the network security that designs and proposes IDS. This is useful for classifying security attacks and creating specific rules for various security attacks. Many rule-based IDS are not easy to detect new attacks. Anomaly based IDS using the concept of genetic algorithm uses a set of classification rules derived from network adult data. By using this function, the quality and reliability of each rule is monitored. Research applying machine learning has been studied as a method to improve performance of IDS and the security of MANET. By applying various classification approaches of machine learning, normal nodes and attack nodes can be classified. There is also a technique proposed for the security of the network layer by applying the SVM classification technique based on the hierarchical architecture and the distributed architecture. A hybrid model based on Bayesian classifier, Markov chain rules and Association rule mining was proposed by [27]. The proposed method

provides security at different layers such as MAC, routing, and application layers. Then, attack nodes are identified by evaluating the characteristics of nodes in different layers.

3. Proposed Efficient Authentication and Distributed Monitoring Techniques

3.1. System Structure

If the reliability of nodes participating in the network is verified and the integrity of transmitted data is guaranteed, the reliability of MANET can be improved. In order to achieve this, in this paper, an authentication technique through efficient trust evaluation and an attack detection technique using a distributed monitoring technique are proposed. The proposed technique applied a cluster which is a hierarchical structure for authentication and distributed monitoring of nodes. Fig. 1 shows the structure of the technique proposed in this paper.

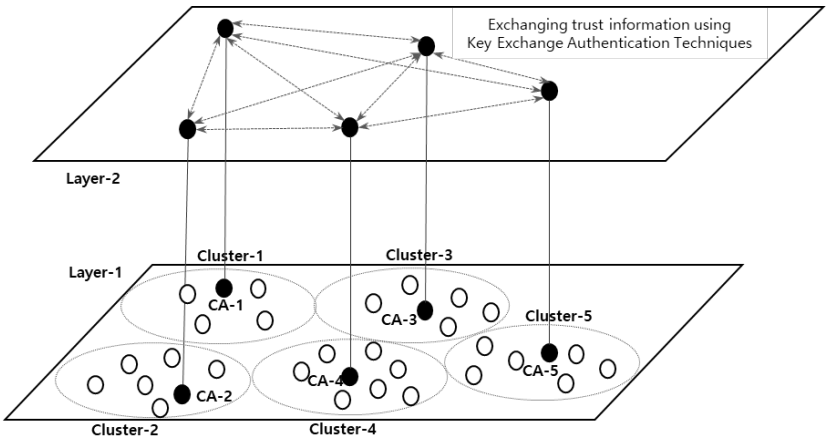


Fig.1. System structure of the proposed technique

The cluster is composed of neighboring nodes with a 1-hop distance, and the node with the highest connectivity among the nodes in the cluster was selected as Certification Authority (CA). The role of CA in each cluster can be classified into node authentication and intrusion detection function. The main role for authentication is table management and trust evaluation. CA manages a Member Key Table (MKT) that manages key to be issued to member node and a Member Trust Table (MTT) that can store measured trust. The trust evaluation is performed by comparing with a reference value after calculating the combination of local trust information directly measured by neighbor nodes and global trust information collected from external clusters. The role of the CA for intrusion detection is to identify the attack node. In this paper, all nodes participating in the network perform monitoring of neighbor nodes at 1-hop distance from themselves and collect packet forwarding, packet generation, and packet discarding information through this. The information collected in this way goes through an attack node determination process step for nodes whose reliability is less than or equal to the standard in the trust evaluation of the nodes. According to the result, the states of the nodes are determined as an attack node, a boundary node, and a normal node. If an attack node is determined, the information of the node registered in MTT is updated and the node information is transmitted to neighbor CAs. And CA delivers information to all nodes in the cluster, and all packets sent and received from the attack node are discarded. By doing this, it was possible to effectively exclude malicious nodes from participating in the network. In the proposed technique, a key exchange technique was applied to improve the integrity of data transmitted between nodes. Key exchange technique between CA and member node, and between CAs applied different method. Key exchange between CA and nodes is accomplished through key issuance by CA, and key exchange between CAs is applied in a way that key distribution is performed without the help of anyone. This made it possible to provide secure communication.

3.2. Member node trust measurement technique

In this paper, the trust evaluation of nodes is performed by CA. To increase the accuracy of node reliability, this measurement technique is calculated by combining local trust (LT) calculated by neighboring nodes and global trust (GT) by previous trust of the node. And this can increase the trust of the nodes and improve the network lifetime.

LT is made by measuring the signal strength between two nodes and the error ratio compared to packet transmission for a certain period of time. In order to obtain the local trust information of node N, Received Signal Strength (RSS) in the neighboring nodes of node N is measured using equation (1).

$$\mathrm{RSS}[\mathrm{dBm}] = \log_{10}\alpha + \theta[\mathrm{dB}] + S_{tx}[\mathrm{dBm}] \tag{1}$$

And the transmission ratio between the nodes are calculated by using equation (2) after measuring received whole

packets and the packets with errors among all packets received from node in a neighbor node for a certain period of time.

$$\mathrm{AVG(ER)} = \sum_{i=1}^{n} MN_i \frac{P_{err}}{P} \tag{2}$$

Here, P is the total amount of packets transmitted between the two nodes, and $P_{err}$is the amount of error packets between the two nodes. The trust of the nodes is determined by the combination of LT calculated by the neighbor nodes and GT of nodes received from the neighbor CA. GT is the average value of the trust evaluated in the cluster that the nodes belonged before. CAs periodically broadcast the trust of nodes in the managing cluster to neighbor CAs. GT and LT collected in this way calculate the trust of the node by equation (3).

$$\mathrm{T(N)} = \frac{RSS_{N_i}}{Avg(ER)} \cdot \omega + GT(N) \cdot (1 - \omega) \tag{3}$$

Here, ω represents the weight for the time the node N entered the cluster. The trust measured in this way is used for authentication of nodes. That is, if the trust of node N is lower than the average trust in the cluster, the cluster key for communication is not issued to the node. If the cluster key is not issued, it is excluded in communication because the received data cannot be verified. And for nodes with low reliability, the attack node determination process described in 3.3 is performed. Fig. 2 shows the structure of MTT for storing and managing the trust of member nodes in CA.

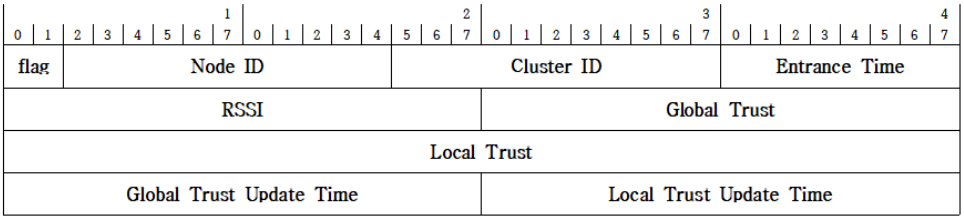


Fig.2. The structure of member trust table

3.3. Cluster key management techniques

All nodes can transmit data only with cluster key issued from CA in order to ensure the integrity of transmitted data. For this, the node requests the cluster key issuance from CA of the cluster to which it belongs. CA requested to issue the cluster from the node checks the trust of the node. If the value is higher than the reference value, the cluster key is issued through the generation process of the key. The cluster key generation is as follows. First, for cluster key issuance, each digit of sequence number of request packet sent by the source node is added, the remainder divided by 10 is calculated, and the key matching the index of cluster key table is transmitted to the source node. The key issued in this way becomes the only key for encryption/decryption of transmitted and received data. If a key is issued in the CA to the source node, the corresponding information is transmitted through encrypted communication. Therefore, all CAs share the issued key information. The source nodes encrypt data to be transmitted to the goal nodes and transmit. It is not easy to modulate this encrypted data because the data is encrypted even if there is a malicious node in the route to the goal node. Even if it is modulated, it has the advantage of strengthening the security of the data because the falsification is detected by checking the integrity using the key in the member node receiving the data. The member nodes received the data transmit Req_CK as a key request packet that the ID of the source node is contained to CA of the cluster by using the key of the encrypted data. The member node receiving the key checks the integrity of the data and the falsification of the data are verified. Fig. 3 shows the process of data transmission and verification using cluster keys.

3.4. Authentication techniques between clusters

The CA manages trust information and node type information for nodes in the cluster, and blocks attack nodes from participating in the network by exchanging information on attack nodes. Therefore, the key exchange authentication technique is applied for secure data transmission with guaranteed integrity in transmitting this important information between CAs. The key exchange technique of CAs is a lightweight authentication technique performed without anyone's help. The goal of this technique is secure and fast key management between CAs. The key exchange process between clusters consists of four steps as follows.

In the first step, the source CA sends its public key and public key authentication signature.

In the second step, the goal CA received the packet transmits a response message including the public key and a hash inspection code (HIC) of the public key.

In the third step, the source CA generates a shared key, encrypts it with the public key of the goal CA, and transmits.

In the fourth step, the data to be transmitted is encrypted and transmitted using the shared key. In this way, the information transmissions between CAs enhance the integrity by providing a secure and rapid authentication method between CAs. And, it is possible to increase the efficiency of each other's key management. Fig. 4 shows the authentication process described above.

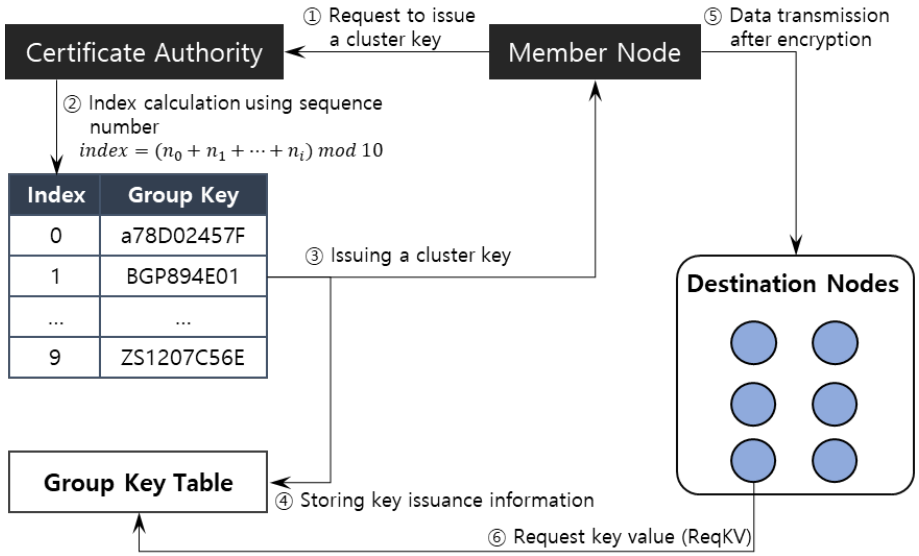


Fig.3. Cluster key issuance and data transmission process

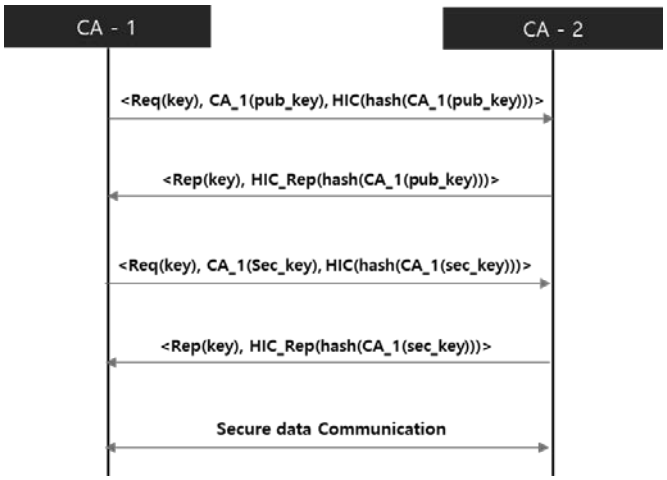


Fig.4. Certification process between CAs

3.5. Intrusion detection techniques

In this paper, a distributed monitoring technique was proposed for efficient detection of malicious nodes and attacks in a dynamic environment. The proposed intrusion detection technique monitors traffic to neighbor nodes within a 1-hop distance from nodes in the cluster. The trust information about neighbor nodes collected from all nodes are managed by CA. CA performs trust management and node class management for nodes in the cluster. For intrusion detection, packet forwarding rate, packet generation rate, and packet discard rate are measured. These measured values are transmitted to their CA. CA compares the average value of the cluster it manages and classifies the node into an attack node, a boundary node, and a normal node according to the result. If an attack node is detected, the node registers with MTT and transmits the attack node information to the neighbor CA and transmits information about the attack node to the entire network. In addition, each CA delivers the attack node information to the nodes in the cluster, discards all packets received from the attack node and blocks all packet forwarding to the attack node. When exchanging trust information about nodes or information about attack nodes between CAs, the authentication technique described in the previous section is applied to block data modulation by attack nodes. Fig. 5 shows the distributed monitoring intrusion detection structure.

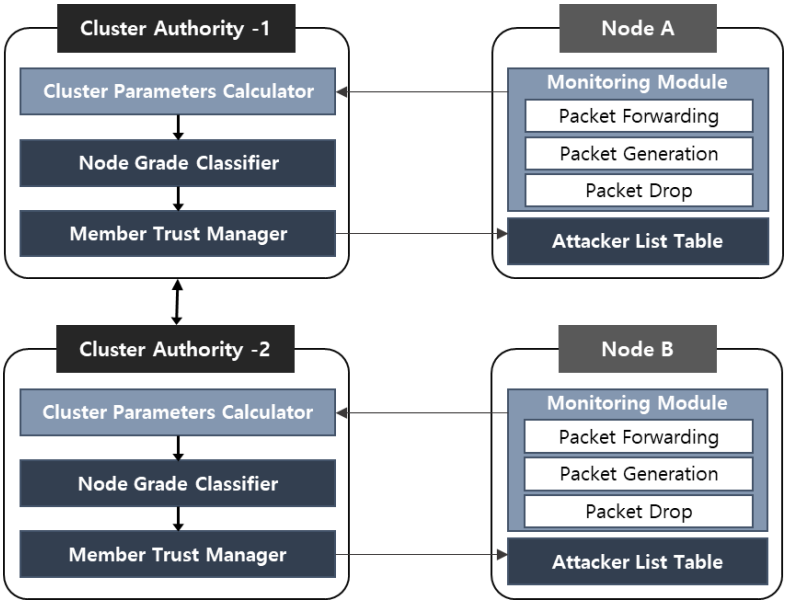


Fig.5. Proposed intrusion detection structure

For intrusion detection, the monitoring traffic for neighbor nodes at 1-hop distance is the packet forwarding rate(P_f), packet generation rate(P_g), and packet discard rate(P_d). The traffic values for each neighbor node at 1-hop distance from itself are measured and stored as a set of properties. The set of properties of node N_i is expressed s equation (4).

$$S_{N_i} = \{P_f, P_g, P_d\} \tag{4}$$

In this way, the activity of the neighbor nodes is monitored, the values of the properties are stored as a multidimensional vector, and the values are transmitted to the CA. The parameters used to determine whether an attack exists in this paper are measured as follows. First, the packet generation rate means a value measured the amount of control packets that node k generates to its neighbor node n for a certain period time. And, the average value of the control packet of the cluster to which node n belongs is measured by equation (5).

$$C_k(Avg(P_g) = \sum_{i=1}^{n} \frac{P_g(N_i)}{n} \tag{5}$$

If the amount of control packets generated by a node n is much larger than the average value in the cluster, the node may suspect a flooding attack. In a multi-hop environment, data transmission must perform in all nodes. The second packet forwarding rate means at which a neighbor node transmits a packet towards the destination node. If this rate is significantly higher than other nodes, the node can be suspected as a selective attack. Therefore, a node $k$to CA of the cluster to CA of the cluster calculates the rate of packets successfully forwarded to its neighbor node $n$for a certain period of time by the following equation (6).

$$P_t = \sum_{t=1}^{n} \left(\frac{P_f(N_k)}{P_r(N_d)}\right) \tag{6}$$

Here, $P_f(N_k)$ is the amount of packets that the node n forwards to the destination node n, $P_r(N_d)$ is the amount of packets that the destination node d is among packets received by the node n. And the average value of packet forwarding within the cluster is calculated in the same way as in equation (5). The third packet discard rate is the value measuring packets forwarded to other neighbor nodes among all packets received neighbor node n. If the value is high, the node can be suspected of being a selfish node. This value is calculated by equation (7).

$$P_d = \sum_{t=1}^{n} \left(\frac{P_f(total)}{P_r(total)}\right) \tag{7}$$

The three parameter values measured in this way are compared with the average values in the cluster measured by the CA and then the flag values for normal (1), suspicious (0), and attack (-1) is set. In node classifier, even if at least one of the three parameters has an attack (-1) flag, the node is classified as an attack node, and if there are two or more suspicions (0), it is classified as a boundary node. If it is determined as an attack node, the information on the node is broadcast to the neighbor CA. The information of attack node is registered in the attack node list of all nodes, and

network participation is excluded by discarding all packets from the node. In the case of suspicious nodes, the number of activity monitoring is increased by increasing the monitoring interval. In this way, the network stability was improved by increasing the accuracy of attack node detection through distributed monitoring of neighbor nodes in each node.

4. Experiments and Results

4.1. Experimental Environment

In this chapter, the main performance of the security method proposed in this paper was evaluated. In order to evaluate the performance of node authentication and attack detection proposed in this paper, ns-2 simulator was used and the experiment was performed in the following environment. The experiment was performed on the intel core i9 CPU and memory 32GB. The mobile node used in the experiment is a random way point model that freely changes location while moving freely in the network. The movement speed of the nodes moves from 0 to 20 in variety. And the battery consumption of the nodes was not considered. The experiment time was set to 300 seconds, and various parameters presented in Table 2. The attack used in the experiment caused a black hole attack and a flooding attack 5 times and the performance of the network was measured at this time.

Table 2. Simulation parameters

Parameter	Value
Network Size	1000 × 1000
Number of Nodes	50, 100
Number of Malicious Nodes	10
Routing Protocol	AODV
Pause Time (Sec)	20
Attack Type	Blackhole, Flooding
Simulation Time	60
Traffic Pattern	CBR
MAC Layer	IEEE 802.11

4.2. Experimental Results

In this chapter, the result of the performance measurement of the attack detection method proposed in this paper is described. The performance evaluation criteria were set processing rate according to the presence or absence of attack, end-to-end delay, packet loss rate, and false positive rate.

Network throughput: It is data packet transmitted between a source node and a goal node for a certain period of time.

End-to-end delay time: The end-to-end delay is averaged over all surviving data packets from the sources to the destinations

Packet loss ratio: The ratio of packets that are not received among the total packets transmitted between the source node and destination node

False positive ratio: The rate reported as an attack but an attack does not actually exist

The performance evaluation of the CA-to-CA authentication method proposed in this paper is replaced with this because important information is exchanged accurately without forgery or falsification by key exchange and the performance for the above-mentioned evaluation criteria is excellent. The performance measurement was comparative experimented with the DLM technique and the SRP technique.

Fig. 6 shows the result of measuring he average rate of packets successfully transmitted to the destination node during unit time. The SRP technique showed good result in terms of throughput because attacks were detected by checking the amount of packets between the source node and the destination node. DLM technique showed good results in packet throughput because control packets were dynamically checked. The proposed technique also showed excellent results even in the presence of an attack because attacks detected by measuring the packet generation, discarding, and forwarding rates generated in the nodes. In the proposed technique, network participation is performed through trust evaluation and authentication of nodes at neighbor nodes, so the packet processing results were good even in the case of an attack.

Fig. 7 shows the result of measuring the time when the data packet generated by source node completely arrived at the destination node. The SRP technique shows a rather high delay time when an attack occurs because the attack detection performance is low by neighbor nodes other than the attack on the path set between the source node and the destination node. The DLM technique shows excellent results for attack detection because attacks are detected by

checking the amount of RREQ and RREP and sequence number for route setting and dynamically update. The proposed technique shows good results even when an attack occurs because attacks of its neighbors are monitored in all nodes.

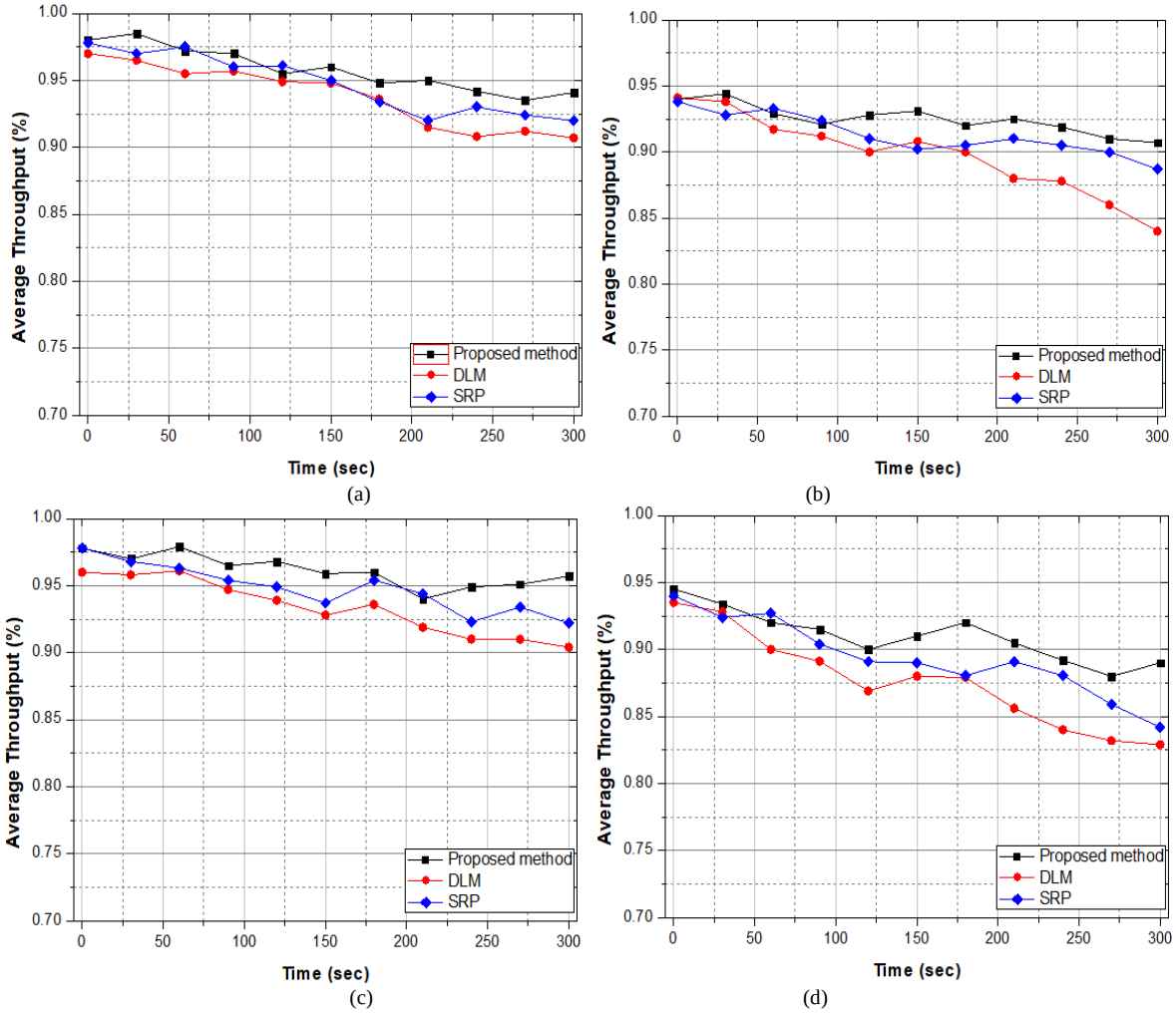
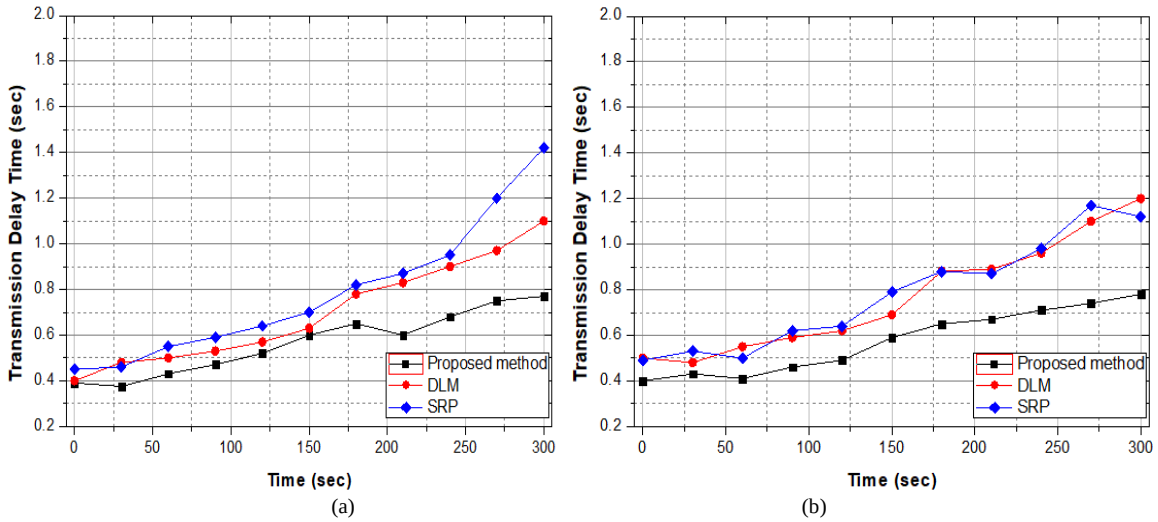


Fig.6. Results of average throughput based on the presence of Blackhole attack and Hello flooding attack (a) Measurement results of 50 nodes without of Blackhole attack and Hello flooding attack; (b) Measurement results of 50 nodes in Blackhole attack and Hello flooding attack; (c) Measurement results of 100 nodes without of Blackhole attack and Hello flooding attack; (d) Measurement results of 100 nodes in Blackhole attack and Hello flooding attack.



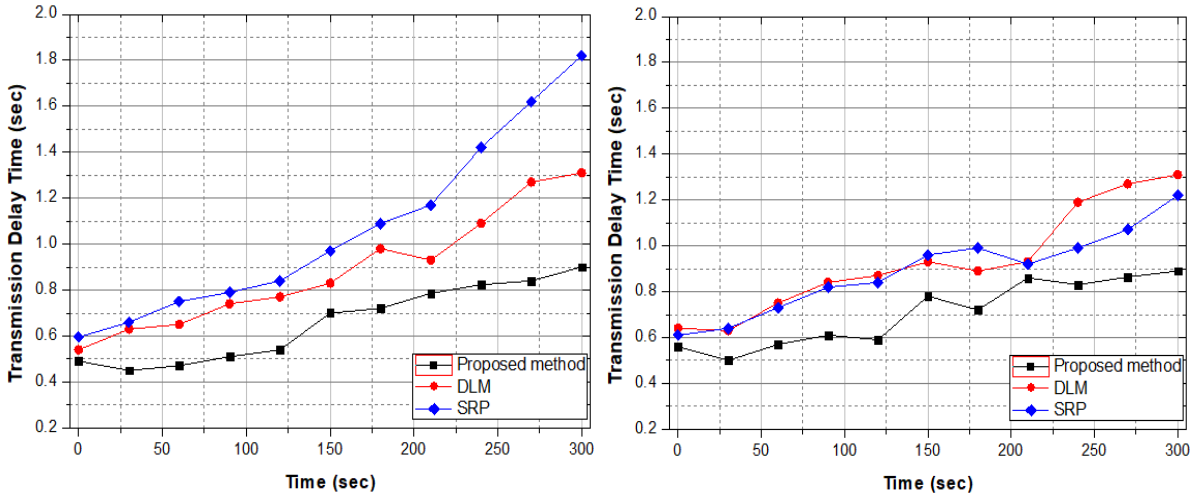


Fig.7. Results of transmission delay time based on the presence of Blackhole attack and Hello flooding attack. (a) Measurement results of 50 nodes without Blackhole attack and Hello flooding attack; (b) Measurement results of 50 nodes in Blackhole attack and Hello flooding attack; (c) Measurement results of 100 nodes without Blackhole attack and Hello flooding attack; (d) Measurement results of 100 nodes in Blackhole attack and Hello flooding attack.

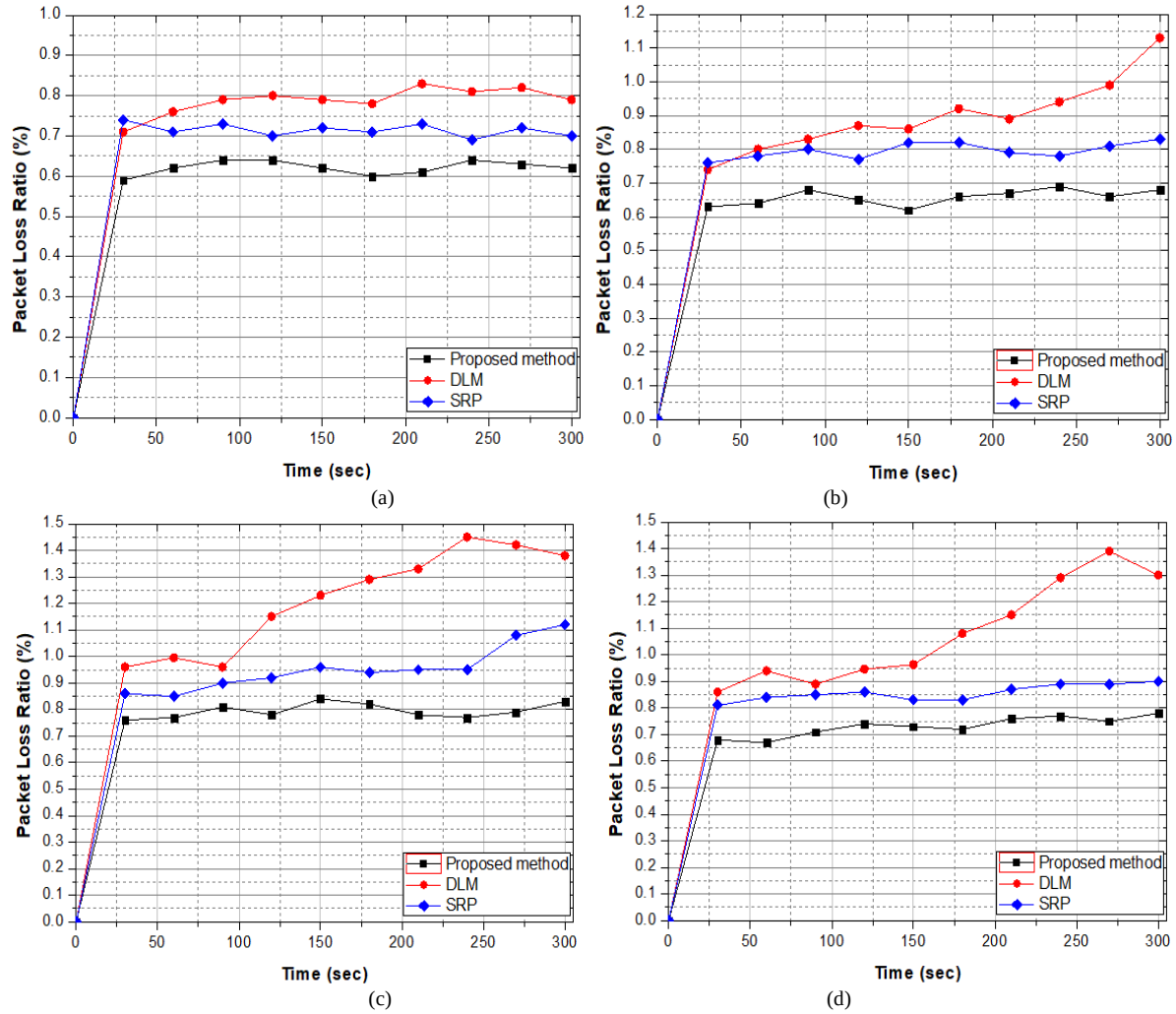


Fig.8. Results of packet loss ratio due to Blackhole attack and Hello flooding attack. (a) Measurement results of 50 nodes without Blackhole attack and Hello flooding attack; (b) Measurement results of 50 nodes in Blackhole attack and Hello flooding attack; (c) Measurement results of 100 nodes without Blackhole attack and Hello flooding attack; (d) Measurement results of 100 nodes in Blackhole attack and Hello flooding attack.

Fig. 8 shows the experimental results in the packet loss rate. This evaluation criterion is an important factor which detects how quickly the attack node and reduces packet loss to the destination node when an attack occurs. SRP

technique shows that packet loss rate is sharply increased as the movement speed is increased because of rerouting by the movement of the node and low detection performance for neighbor nodes. DLM technique shows good performance by rerouting in spite of occurring of attack because it performs attack detection through dynamic update. The proposed technique shows a rather high packet rate by the movement speed of the nodes. But it was confirmed that the presence or absence of an attack was not significantly affected and the packet loss rate is a factor which shows that the attack detection performance is excellent.

The false positive ratio is one of the most important performance evaluation factors of intrusion detection. Fig. 9 shows the average value of the result of 10 repeated experiments for the black hole attack and the flooding attack used in the experiment. As shown in the Fig. 9, the proposed technique has a significantly lower false positive rate compared to the other two techniques because all nodes monitor neighbor nodes at 1-hop distance and information is managed. The average false positive rate of the proposed technique was 3.3%, and the SRP technique showed 4.26%. The SRP technique showed that the false positive rate increased because attack detection was performed by comparing only the number of packets sent and received.

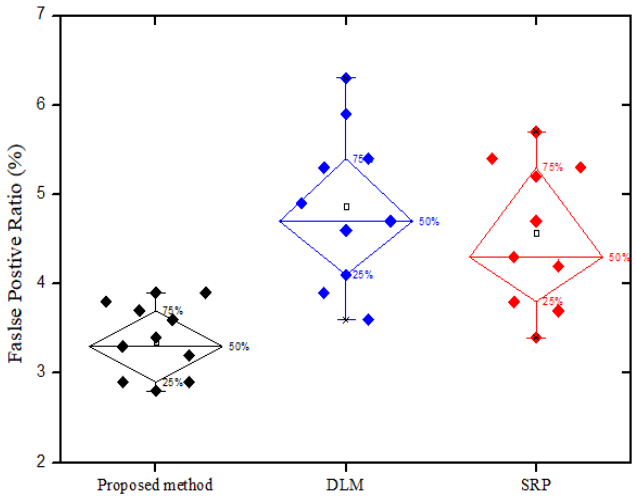


Fig.9. Results of false positive ratio due to Blackhole attack and Hello flooding attack.

5. Conclusions

A routing protocol creating the most efficient route is required because MANET utilizes dynamic topology and limited resources. In addition, authentication method for nodes participating in such routing and blocking the participation of malicious nodes is very important in terms of network reliability.

Therefore, this paper was focused on increasing the authentication method for nodes to improve network reliability and the efficiency of attack to detection, having the ability to detect multiple attacks at the same time, and reducing the false positive rate. First, in order to provide accurate authentication for nodes, the local reliability measured directly by neighbor nodes and the global reliability value measured reliability value in the previous cluster of nodes was combined. And more accurate reliability measurement method was provided to weigh according to the time the nodes participate in the network. In particular, the local reliability was able to determine the selfish behavior of the nodes because it is measured based on the signal strength and packet transmission rate between the nodes.

And for intrusion detection through the distributed monitoring technique, the packet forwarding rate, packet generation rate, and packet discard rate were determined as attack detection parameters. For distributed detection, information was collected from all nodes participating in the network through monitoring traffic to neighbor nodes at 1-hop distance. A cluster structure was used to efficiently manage the collected information and determine whether an attack occurred. The CA applied the detection algorithm the parameter attribute values collected from the node, and performed the role of a central administrator such as judging the attack node and managing the trust information of the nodes. In addition, it is inevitable to consider alteration of transmission information by malicious nodes when exchanging attack node information and trust information between CAs. Therefore, the fast and secure data transmission technique was proposed using only the key exchange between nodes consisting of four steps. Through this process, the efficiency of key management was improved, and the integrity of the trust information of the attack node and the nodes was provided. The proposed in this paper was comparative experimented by using the throughput, packet loss rate, end-to-end delay, and false positive rate according to the number of nodes and attacks as performance evaluation criteria. The excellent performance of the proposed technique was confirmed through experiments. The goal of this paper is to reduce damage even if an attack occurs on the network and to increase the safety of the network by including malicious nodes from the network. Through the experiment, it was confirmed that the proposed distributed monitoring technique and node authentication technique detect attack nodes more than 95% on average. Future research

will greatly improve attack detection performance if a learning model based on network traffic is established and attack detection and classification based on it is performed.

Acknowledgments

This paper was supported by Joongbu University Research & Development Fund, in 2020.

References

[1] Kukreja, D., U. Singh, and B. Reddy, “A survey of trust based routing protocols in MANETs,” Journal of Advances in Computer Networks, 1(4), 2013, pp. 280-285.
[2] Del-Valle-Soto, Carolina, Mex-Perera, Carlos, Monroy, Raul, Nolazco-Flores, Juan Arturo, “On the routing protocol influence on the resilience of wireless sensor networks to jamming attacks,” Sensors, Vol. 15, 2015, pp. 7619-7649.
[3] Saudi, N.A.M., et al., “Mobile Ad-Hoc Network (MANET) Routing Protocols,” in Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017): Transcending Boundaries, Embracing Multidisciplinary Diversities, Springer, 2019.
[4] Das, M. Venkat, P. Premchand, and L. R. Raju., "Security Enhancing based on Node Authentication and Trusted Routing in Mobile Ad Hoc Network (MANET)," Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.14, 2021, pp. 5199-5211.
[5] Singh, V.; Singh, D.; Hassan, M.M., “Survey: Black Hole Attack Detection in MANET,” In Proceedings of the 2nd International Conference on Advanced Computing and Software Engineering (ICACSE), Sultanpur, India, 8–9 February 2019.
[6] Yang, Hwanseok, "A Study on Improved Intrusion Detection Technique Using Distributed Monitoring in Mobile Ad Hoc Network," Journal of Korea Society of Digital Industry and Information Management 14.1, 2018, pp. 35-43.
[7] Kaur, Gunseerat, and Poonam Thakur., "Routing Protocols in MANET: An Overview," 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Vol. 1, IEEE, 2019.
[8] Saudi, N.A.M., et al., “Mobile Ad-Hoc Network (MANET) Routing Protocols,” in Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017): Transcending Boundaries, Embracing Multidisciplinary Diversities, Springer, 2019.
[9] Mohamed, Salma S., A. I. Abd-Elfattah, and Mohamed A. Mohamed. "A new clustering technique based on replication for MANET routing protocols." TELKOMNIKA 18.6, 2020, pp. 3339-3345.
[10] Yadav, Neha, and Urvashi Chug., "Secure Routing in MANET: A Review," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon). IEEE, 2019.
[11] Moudni, H., et al., “Performance analysis of AODV routing protocol in MANET under the influence of routing attacks,” in 2016 International Conference on Electrical and Information Technologies (ICEIT), IEEE, 2016.
[12] Prasath, N., and J. Sreemathy, "Optimized dynamic source routing protocol for MANETs," Cluster Computing 22.5, 2019, pp. 12397-12409.
[13] Wahi, Charu, Shampa Chakraverty, and Vandana Bhattacherjee, "A trust-based secure AODV routing scheme for MANET," International Journal of Ad Hoc and Ubiquitous Computing 38.4, 2021, pp. 231-247.
[14] Jain, Pragati, and Akash Sanghi, "Review of Various Routing Protocols in Mobile Adhoc Networks (MANETs)," International Journal of Innovations & Advancement in Computer Science, 2018, pp. 45-54.
[15] Bhardwaj, Diwakar, Krishna Kant, and Durg Singh Chauhan, "QoS-aware routing protocol using adaptive retransmission of distorted descriptions in MDC for MANETs," International Journal of Ad Hoc and Ubiquitous Computing 28.1, 2018, pp. 55-67.
[16] Halhalli, Suresh R., Shounak Rushikesh Sugave, and B. N. Jagdale, "Optimisation driven-based secure routing in MANET using atom whale optimisation algorithm," International Journal of Communication Networks and Distributed Systems 27.1, 2021, pp. 77-99.
[17] Ram, Anant, Jagrati Kulshrestha, and Vishesh Gupta, "Secure Routing-Based AODV to Prevent Network from Black Hole Attack in MANET," Proceedings of 6th International Conference on Recent Trends in Computing. Springer, Singapore, 2021.
[18] Alappatt, Valanto, and Joe Prathap PM. "Trust-Based Energy Efficient Secure Multipath Routing in MANET Using LF-SSO and SH2E." International Journal of Computer Networks and Applications 8.4, 2021, pp. 400-411.
[19] Li, Xiaochen, et al. "Secrecy transmission capacity in mobile ad hoc networks with security-aware Aloha protocol." IET Communications 14.22, 2020, pp. 4135-4141.
[20] Kim, Jinhong, and Jong-Yun Kim, "Wireless Ad Hoc Network based Routing Attack Authentication Mechanism." Advances in Natural and Applied Sciences 14.1, 2020, pp. 224-230.
[21] Kamboj, Nippun, and Munishwar Rai, "A new secure ad-hoc on demand distance vector routing protocol to ensure less power consumption in mobile ad-hoc network," Journal of Computational and Theoretical Nanoscience 17.6, 2020, pp. 2483-2487.
[22] Barik, Lalbihari, "A Survey on Detecting Co-Operative Black Hole Attack on Multicast in Mobile Ad-Hoc Network," International Journal of Current Engineering and Scientific Research 5.11, 2018, pp. 149-155.
[23] Desai, Aneri Mukeshbhai, and Rutvij H. Jhaveri, "Secure routing in mobile Ad hoc networks: A predictive approach," International Journal of Information Technology 11.2, 2019, pp. 345-356.
[24] Gupta, Prakhar, et al., "Reliability factor based AODV protocol: Prevention of black hole attack in MANET," Smart Innovations in Communication and Computational Sciences. Springer, Singapore, 2019, pp. 271-279.
[25] Panda, Niranjan, and B. Kumar Pattanayak. "Energy aware detection and prevention of black hole attack in MANET." International Journal of Engineering and Technology (UAE) 7.2.6, 2018, pp. 135-140.
[26] Suma, R., B. G. Premasudha, and V. Ravi Ram. "A novel machine learning-based attacker detection system to secure location aided routing in MANETs." International Journal of Networking and Virtual Organisations 22.1, 2020, pp. 17-41.

[27] Farheen, NS Saba, and Anuj Jain, "Improved Routing in MANET with Optimized Multi path routing fine tuned with Hybrid modeling," Journal of King Saud University-Computer and Information Sciences (2020).

Authors' Profiles

Dr. Hwanseok Yang is an associate professor in the Department of Information Security at Joongbu University. From 2007 to 2010, he served as a research professor in the Cyber Investigation Police Department at Howon University. He received his PhD in Computer Science and Statistics from Chosun University in 2005. He has over 20 years of teaching experience, conducting research in the field of intrusion detection and authentication of computer systems and mobile networks. He currently conducts various researches in the field of using artificial intelligence for intrusion detection.

How to cite this paper: Hwanseok Yang, "A Study on Performance Improvement of Intrusion Detection using Efficient Authentication and Distributed Monitoring", International Journal of Computer Network and Information Security(IJCNIS), Vol.14, No.2, pp.1-13, 2022. DOI: 10.5815/ijcnis.2022.02.01