International Journal of Multimedia and Ubiquitous Engineering
Vol.10, No.7 (2015), pp.277-284
http://dx.doi.org/10.14257/ijmue.2015.10.7.29

Authentication Techniques for Improving the Reliability of the Nodes in the MANET

Hwan-Seok Yang

Dept. of Information Security Engineering, Joongbu University
Geumsan-gun, Chungnam, Korea
yanghs@joongbu.ac.kr

Abstract

The open structure of MANET, dynamic topology, and infrastructure mobile nodes constituting are threated from many types of attacks. Therefore, what increases the reliability between the mobile nodes and provides efficient routing is an important part to influence network performance. Attack by malicious nodes presenting within the network destructs communication path or discards the packet and the damage is very large. However, it is not easy to detect attacks using these properties. In this paper, we propose an authentication technique to provide secure communication through secure routing scheme for safe data transmission between the nodes and exhaustive reliability testing. Cluster structure is used for authentication technique of the proposed technique and cluster head acts as a certificate authority and is managed authentication information of member nodes. The performance of the proposed technique was confirmed by experiments.

Keywords: *Authentication; Cooperative Security; Network Security; MANET*

1. Introduction

The application fields of MANET have become very diverse as rapid progress of wireless network technology and the spread of wireless devices are widely. MANET has the advantage which can quickly build a network with only nodes without any network infra [1]. But, Network composed without the help of any infra has many security threats. In particular, the dynamic topology by movement of node is difficult to set the path for data transmission and is often the cause of a variety of attacks. Security threats related to the routing mechanism have the most type of attack and the damage is also the largest. All nodes constituting a network should act as a router. But, it is possible to cause a variety of attacks such as black hole and DoS because difficult path setup and maintain by the movement of the nodes and malicious nodes on the path involves [2-3]. The performance of the entire network will be low by interrupting the flow of data between nodes. Therefore, the authentication service that can increase the reliability between the nodes must be provided in order to defend such attack. On MANET, the fixed CA (Certificate Authority) issues certificates as in a wired network environment and cannot manage this. It is not easy to also select the nodes to perform the CA role. The technique that can block this is necessary because the wrong authentication can be done by malicious nodes in the key management mechanism using for the authentication of nodes.

In this paper, we propose a multi-factor authentication technique in order to improve the secure routing technique and reliability for safe data transmission between nodes. We use the cluster structure for authentication of nodes and the cluster head managing each cluster is elected by combining the reliability of nodes and the number of connections. The node with the highest value in the elected cluster head like this performs CA role. The node elected to cluster head manages the MAT (Member Authentication Table) in order to save certificate issued information issued to member nodes and trust information.

ISSN: 1975-0080 IJMUE

Member node within cluster can transmit data only when it have a certificate issued by CA and provide secure routing by excluding the full participation of nodes that do not issue a certificate, namely have low reliability in network.

This paper is organized as follows. The existing secure routing and authentication technique is described in chapter 2 and secure routing and authentication technique for proposed reliability improvement in this paper is described in chapter 3. The performance of the proposed technique is evaluated through experiments in chapter 4. Finally, chapter 5 concludes.

2. Related Works

2.1. Secure Routing Protocol

The routing protocol can operate normally under the assumption with the confidence for each mobile node. This causes many security problems like packet loss or destruction of the network if a malicious node in the path set camouflages and participates [4]. There are proposed many techniques like SAR, ARAN, and SRAODV to solve the structural problems of these routing techniques.

SAR (Secure Aware Routing Protocol) technique sets the path using the trust level of the nodes [5]. If the node has low confidence level is found between the source node and the destination node, new path is built without using the path and a potential risk by unreliable nodes are blocked in advance.

ARAN (A secure Routing protocol for Ad hoc Networks) technique provides a much enhanced security by using authentication between the source node and the destination node and link authentication between nodes. This technique has the authentication server and nodes participating in the network should be issued certificate from the authentication server. The source node signs RREQ message and certificate to secret key and broadcasts for the path search. The destination node subscribes RREP and certificate to secret key and transmits to the source node. End-to-end authentication is provided and the verification process for the intermediate nodes provides the authentication between links because the source node determines the validity of the path reply packet only with public key of the destination node [6].

SRAODV (Secure Routing with AODV) is the technique which ensures the safety to AODV as avoiding formation of routing loops and redirection prevention of the minimum path by being participated only certified nodes to path set [7]. All nodes must obtain the public key from the CA and then generates a group session key between neighbor nodes before they participate in the network. Routing and data forwarding performs using this session key. This provides authentication by key exchange and provides integrity, non-repudiation, *etc*. However, this has disadvantage that resources waste of intermediate nodes transmitting the packet is caused if a malicious node copies packet received from the source node and transmits.

2.2. Authentication Techniques

In MANET, an authentication technique to provide confidence for nodes has been studied. Self-organized way in these authentication techniques is that node itself issues certification and cancels. In this point, this technique is similar to Pretty Good Privacy (PGP) technique [8]. However, these are difference in the method that stores and distributes certification. Therefore, every node is necessary memory space to store certification of each node. Each node stores the path of their neighboring node as a graph format. The beginning of each path is the node itself and if the certificate chain is present in the graph, this means that can reach the node.

Polynomial Secret Sharing (PSS) technique as a distributed authentication service technique is that a node cannot provide complete authentication service and is capable

only after an electric signature distributed to multiple nodes gathers [9]. This technique has certification certified by a certificate signing key sharing with each other and certification can be verified at any place because it assumes that this public key is known to all nodes. Therefore, a complete certification cannot be produced unless the confidence of k nodes in their surroundings is received and if a certificate is not had, it is included because of regarding as the attacker. But, the update of certificate is not possible in a situation that k nodes around the node don't exist [10]. Figure 1 is shown the process generating the certification from node in the PSS technique.

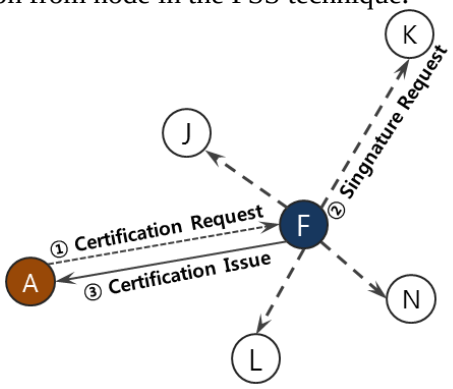

Figure 1. PSS Authentication Process

3. Proposed Authentication Method

In this chapter, we propose secure routing technique for high safety of data transmission between nodes and an authentication technology for nodes to improve the reliability of the network. The proposed technique in this study improves the overall performance of network by improving performance of authentication technology and reducing network traffic using hierarchical structure.

3.1. Network Architecture for Authentication

In this paper, the cluster of hierarchy structure is used to evaluate confidence of all nodes in the network. The cluster head is elected by using confidence value among the nodes in the cluster and node which has the highest value among the elected cluster heads performs CA role. Here, confidence value is a ratio of delivering the packet to neighbor nodes of the nodes and confidence value of nodes participating for the first time in the network will have the initial value 0. The confidence value indicates that each node is not selfish and how it participates to deliver packet. This is used as a measure showing the confidence relationship between nodes. Figure 2 is shown the network structure for the authentication used in this paper.

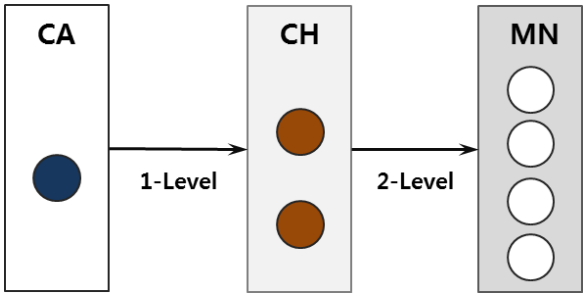

Figure 2. Network Structure for Node Authentication

3.2. Election of CA

The election of cluster head which evaluates the confidence of member nodes within a cluster and issues the certificate may be very important. This is because cluster head can exclude network participation of malicious nodes depending on whether trust for the member nodes and certificate issue. All nodes within a cluster transmit confidence value of the neighboring nodes with HELLO message. Here, trust value is the ratio involved in packet transmission and has a value between 0 and 1. The highest node among broadcasted trust information values is selected as the cluster head. The highest node in the elected cluster head is elected as CA. A store the information in the certification management table in order to manage the certification information issued to each cluster head. The cluster head stores the information in member authentication table in order to manage authentication key issued to member nodes. The structure of CMT (Certificate Management Table) is shown in Figure 3.

Node ID	Request Time	Certificate Time	Public Key
5	15:21:10	15:21:25	P(CA,CH5)
1	15:50:33	15:51:02	P(CA,CH1)
...	...	...	...
6	16:01:21	16:01:40	P(CA,CH6)

Figure 3. The Structure of CMT

3.3. Node Authentication and Secure Routing

The multi-steps authentication technique is used for authentication of the member nodes by trust check. First, the node had the highest confidence value among the cluster heads performs CA role. Each cluster head asks CA to issue certification after it creates the paring-based cryptographic key pair. CA asked certification issue from cluster head issues certification after it identify cluster head. The cluster head performs validation by verifying certification issued. Only cluster head issued certification can perform the authentication key request from the member nodes within the cluster. The authentication key request process of member node in cluster head is as follow. First, cluster head creates member node public key (Pch1, M1) using a hash function. And then, member node secret key (Sch1, M1) is created. The member nodes issued authentication key pair from cluster head indicates CH1, M1 and this means member node Mi issued by cluster head Chi. Figure 4 is shown the issued process of authentication key by the member node as described above.

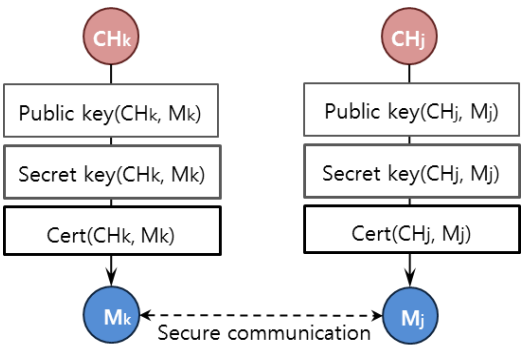

Figure 4. The Process of Certificate and Secure Communication

Member nodes can participate to network only with issued certificate from cluster head. Cluster head has CMT for the trust evaluation of the member nodes within cluster and updates trust information of member nodes. The structure of MAT is shown in Figure 5.

Node ID	Trust	Location Info	Certificate Time	Start Time
4	0	7 2	21:09	20:54
2	1	1 5 4	19:57	19:54
...	...	...	...	...
7	0.5	7 4 5 6 3	18:11	18:10

Figure 5. The Structure of MAT

In the Figure 5, location info field indicates the cluster information that the node and this information is utilized to figure out the location of malicious nodes. If a particular node k moves to cluster 11, the node k requests a certificate issued to cluster head of cluster 1. The cluster head of cluster 1 broadcasts trust information of node k to the neighboring cluster heads in order to process this request. If the trust value of node k is over reference value which trusts nodes, a certificate is issued. Otherwise, the certificate is not issued. Member nodes which are not issued a certificate like this cannot transmit data and should be high trust value by participating to transmit data. If trust information of node k is not received from neighboring cluster head, it is judged that the node participates first in the network and the node value in MAT is initialized and stored. The certificate of node k is not issued. The reliability is again measured and whether the certificate of node issues is determined after the time to participate in network is provided for a certain time. Member nodes provides non-repudiation function when it transmits data using authentication key issued from cluster head and the reliability of communication can be improved through more stringent authentication.

4. Experiment and Result

4.1. Simulation Environment

In this chapter, we evaluate the performance of secure routing technique applied the multi-factor authentication in this paper. The ns-2 simulator is used for performance evaluation and the experiments are carried out in the following environment. First, the size of network used in the experiments is 1500m×1500m, the transmission range is 200m, and experiment time is 300seconds. Mobile node model used in the experiment is random-way point model and moves at a speed between 0 ~ 20m/s. The malicious nodes are 10 and generated a flooding attack randomly 10 times. Table 1 shows the environment parameters used in the experiment.

Table 1. Environment Parameters

Parameter	Value
Number of Nodes	100, 200
MAC Protocol	IEEE 802.11 DCF
Packet Rate	4 packets/sec
Malicious Node	10, 20

4.2. Simulation Result

In this paper, we measured the superior routing performance and authentication reliability of the proposed techniques through comparative experiments with ARAN technique. The standard of performance evaluation is FRR (False Reject Rate) in order to measure accuracy of data transfer rate, issued rejection ratio of authentication key, and the confidence evaluation.

The issued reject ratio of authentication key is measured in order to confirm the performance of proposed authentication technique in Figure 6. That is, how exactly confidence evaluation of member nodes in cluster head is performed is confirmed. Malicious node can be completely ruled out the network by not issuing an authentication key to malicious nodes. It is confirmed that the proposed authentication technique has stable performance without being influenced by the moving speed and the number of nodes.

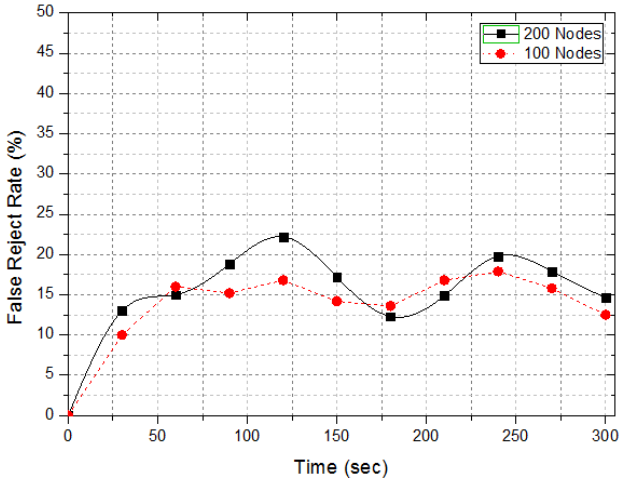

Figure 6. FRR by the Number of Nodes

In the Figure 7, the data transmission rate is measured at situation that malicious node among 100, 200 nodes present 10, 20. The measurement standard is to evaluate the security performance setting the path excluding and avoiding malicious nodes. The ARAN technique shows a poor performance results due to distribution problem of public key for authentication by moving of nodes and difficulty of selection of trusted authentication server. The proposed technique shows the excellent performance because path set is done through the authentication using MAT which cluster heads manage.

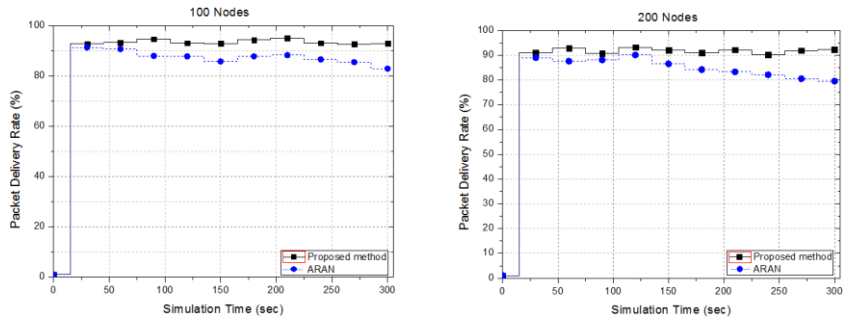

Figure 7. Packet Delivery Rate by the Number of Nodes

Figure 8 shows the measurement result of delay time taken to transfer the data from the source node to destination node. The performance standard id to evaluate the excellence of path set of routing protocol. The ARAN technique shows long delay time because each node should have the public key and the process authenticating each other is required. The proposed technique short delay time of data transfer because only trusted nodes issued certificate perform routing.

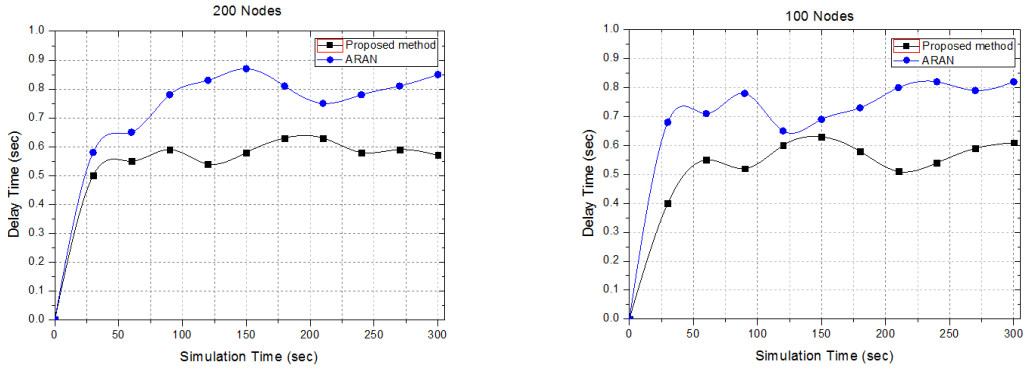

Figure 8. The Delay Time of Data Transfer

5. Conclusion

Recently, popularity of MANET is increasing day by day with the growing application fields of MANET. Especially, the biggest attraction of MANET is that it can construct network quickly with only mobile node without the help of any infrastructure. But, attack threats using vulnerability of the wireless medium and the movement of the nodes are also increasing. The existing routing techniques cannot be applied due to the dynamic topology by mobility of nodes and it is necessary to security techniques for routing attacks that can wreak havoc to network–wide. In particular, mutual authentication mechanism which can provide confidence of nodes is essential. Therefore, we applied a multi-steps authentication technique for accurate authentication of the mobile nodes in this paper. The node with the highest confidence value among the cluster heads performs CA role and issues certificate to each cluster head. The cluster head issued the certificate from CA issues authentication key by measuring the reliability of their member nodes. In this way, it is possible to perform data transfer only after member nodes receive the authentication key. The confidence value of member node could improve the accuracy more by using a confidence value collected from surrounding neighboring nodes to issue an authentication key. The excellent performance of secure routing and authentication technique proposed in this paper is confirmed through comparative experiments with ARAN technique.

References

[1] Kamanshis B., Md L. A., "Security Threats in Mobile Ad Hoc Network," **(2007)**.
[2] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 44 no. 5, **(2004)**, pp. 643-666.
[3] K. H. Hsia, M. Y. Chen and M. C. Chang, "Comments on data pre-processing for grey relational analysis," Journal of Grey System, vol. 7 no. 1, **(2004)**, pp. 15-20.
[4] B. Lim and Md. S. Uddin, "Statistical-based SYN-flooding detection using programmable network processor," In Proceedings of ICITA'05, vol. 2, **(2005)**, pp. 465-470.
[5] Y. -C. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 02), IEEE Press, **(2002)**, pp. 3-13.
[6] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attack and Countermeasures," Journal of Ad Hoc Networks, vol. 1 no. 2, **(2003)**, pp. 293-315.

[7] Mulert J. V., I. Welchn and W. K. G. Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV," Journal of Network Computing Application, vol. 35, **(2012)**, pp. 1249-1259.
[8] Babu B. S. and Venkataram P. "A dynamic authentication scheme for mobile transactions," International Journal on Network Security, **(2009)**.
[9] L. Rokach and O. Maimon, "Top-down induction of decision trees classifier – a survey," IEEE Trans. on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 35, no. 4, **(2005)**, pp. 476-487.
[10] S. Capkun, L. Buttyan and J. Hubaux, "Self-Orgranized Public-Key Management form Mobile Ad Hoc Networks," IEEE Trans on Mobile Computing, vol. 2 no. 1, **(2003)**, pp. 52-64.

Author

Hwan-Seok Yang, he is holding Assistant Professor Position in Information Security at Joongbu University. In 2007-2010, he worked as a Research Professor in Dept. of Cyber Investigation Police at Howon University. He received the Ph. D. degree in Computer Science and Statistics from the Chosun University in 2005. He conducts research in the general areas of security analysis of computer system and mobile networks.

