A New Routing Static Information Protection Protocol on Ad Hoc Network

Wen-Chung Kuo[1,*], Jing-Hung Chen[2], and Chi-Sung Laih[2]

[1]Department of Computer Science and Information Engineering,
National Formosa University
Yunlin, Taiwan, R.O.C.
E-mail: simonkuo@nfu.edu.tw

[2] Department of Electronic Engineering, Institute of Computer & Communication
National Cheng Kung University
Tainan City, Taiwan, R. O. C.

Received 2 April 2007; Revised 29 April 2007 ; Accepted 2 June 2007

Abstract. Ad Hoc network is more convenient and cheaper than the networks with infrastructure in the usage and setup. As to wire network, the router and the terminals are also existed in Ad Hoc network. Compared with the roles of nodes in wire network, the major differences are which act two different roles meanwhile in Ad Hoc network. In practice, it is not only to research in communication security but also to setup the correct route becomes a very important subject. In this paper, we propose a new secure routing protocol based on ID-MAC (Identity-Based Message Access code). According to our analysis, this scheme can prevent the problems of routing forging, modifying, and identity authentication on the Ad-Hoc network. Furthermore, we use NS2 (Network Simulator) to simulate our scheme and discuss how well the efficiency is from the simulation results.

Keyword: Ad Hoc network, AODV, ID-MAC.

1 Introduction

The common mobile network usually appears in forms, such as the cellular network or the wireless local area networks. Among cellular network, communication of portable terminal must finish with the aid of base station and switching of portable exchanger; in the wireless local area network, the portable terminal is connected to an existing infrastructural network through the wireless access point. However, today’s cellular networks use fix infrastructures, which are vulnerable to some special environments or the emergency such as the search and rescue after nature calamity. As a consequence, in such conditions, we need to rely on a kind of mobile communication network technology as the Ad Hoc network which individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Furthermore, it requires no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed in the Ad Hoc network. They can be used in many special applications such as military usage, sensor networks, urgent and sudden occasion, remote open-air area, interim occasions, personal communication, and business application.

Until now, many routing protocols of Ad Hoc network are proposed [1], [2], [3], [4], [5], [6]. Compared with other traditional communication networks, there are several characteristics such as without a pre-existing infrastructure, dynamic topologies, dispose automatically, transmission bandwidth-constrained, and energy-constrained operation in Ad Hoc network. Unfortunately, most of authors design originally routing protocols which mainly rely on the efficiency of the routing protocol and the quality of transmission of data. They do not consider the secure problem in the Ad Hoc network. Therefore, many experts and scholars have proposed different solutions to solve the secure problem in the Ad Hoc network [7], [8], [9], [10], [11].

According to our analysis, there are several difficult problems to reach the secure respect in these proposed Ad Hoc networks protocols. First, it is the key distribution problem between nodes. Generally, the authors have all supposed that the nodes already shared a common key each other or obtained others' public keys in advance. Secondly, in the Ad Hoc networks, the malicious node easily modifies the routing information or masks other nodes to forge routing information. How to protect the routing information and authenticate the identity is

[*] Correspondence author

another difficult problem. In some papers, the authors do not particularly describe about their attack models, and not mention how much the influence degree is while the malicious nodes attack the network. Therefore, we need a secure scheme to solve these problems, and a completely attack scenarios analysis and simulation.

In this paper, we will propose a secure routing protocol for Ad Hoc network. Then, we will check this scheme whether it reaches our secure demand. At the same time, we will simulate two attack scenarios to this proposed scheme to verify the influence on Ad Hoc network.

This paper is organized as follows: In Section 2, we will briefly review the Ad Hoc routing protocol, and then the category of attacks in Ad Hoc networks are discussed in Section 3. A new routing protocol based on ID-MAC is presented in Section 4 while the security of this proposed protocol is discussed in Section 5. In Section 6, there are two simulation scenarios and results and our conclusions are presented in Section 7.

2 A Review of Ad Hoc Routing Protocol

Recently, many kinds of Ad Hoc network routing protocols have been proposed. These routing protocols for Ad Hoc networks can generally be divided into three major categories: (1)Proactive route protocol, (2)Reactive route protocol, and (3)Hybrid routing protocol, as shown in Table1. Now, we briefly explain these three routing protocols.

2.1 Proactive Routing Protocols

The Proactive routing protocol is also called table driven routing protocol, i.e., it attempts to maintain consistent and up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond topology changes by propagating route updates. Therefore, it can maintain a consistent network view. Usually, these kinds of routing protocols are revised from existing routing protocol of wired networks.

Although time delay in proactive routing protocol is relatively small, this protocol also needs to maintain and update the route information among each node at any time. Furthermore, this update action will cause the use of network bandwidth inefficient. The famous proactive routing protocols are DSDV (Destination Sequence Distance Vector) [5][10], HSR (Hierarchical State Routing) [6], WRP (Wireless Routing Protocol) [6], etc.

2.2 Reactive Routing Protocols

The Reactive routing protocols are also called on demand routing protocols. It is a kind of routing protocol that discovers the routing path just when nodes need it. Nodes do not have to maintain the accurate routing information in time. In other words, one node will initiate the routing discovery when it needs to send data to an unknown destination. Compared with proactive routing protocols, the consumption of reactive routing protocols is smaller. However, its data transmission latency is bigger. Therefore, it is not suitable for instant applications. The famous reactive routing protocols are AODV, DSR (Dynamic Source Routing), TORA (Temporally Ordered Routing algorithm), etc.

Two major parts, the routing discovery procedure and the routing maintenance procedure, are in AODV [4]. Now, we explain these two procedures as follows.

(1) Routing discovery procedure:

There are two kinds of actions in this procedure.

- Routing Requests (RREQs)

  When one node wants to send a packet to another node (destination), it checks its routing table whether it has a routing path to the destination. If there is no path available, this node will broadcast a RREQ to discover a new path. When a node receives the RREQ, it first checks whether it is the destination. If the answer is no, it checks whether there is a "fresh enough" route to the destination node. If the answer is still no, it will re-broadcast the packet.

  What is a "fresh enough" route? A "fresh enough" route is a non-expired routing entry to a destination, and it uses the sequence number to judge whether it is a "fresh enough" route or not. Only when current sequence number in node's routing table is equal or bigger than the sequence number in the RREQ packet, it is a "fresh enough" route.

- Routing Replies(RREPs)

  When intermediate node receives a RREQ, and it finds that the destination address in the RREQ is itself, it modifies its routing table according to the RREQ. Furthermore, every node receives this RREQ request; it caches the reverse route to the source. The RREP is sent back from the destination node or any intermediate node which satisfies the request to the source node by using the unicast method. Nodes in this path also need to modify their routing table according to the RREP. Finally, the routing table in source node would have the entry to the destination node. After that, data packets can begin to transmit between source and destination.

(2) Routing maintenance procedure:

- Routing Errors (RERRs)

  One node will send RERR messages under the following two conditions:

  1. If a node detects an active route in its routing table and it can not connect to the next hop of this route.
  2. If a node receives a data packet which is sent to another node, but it has no active route to send this packet.

- Use of hello messages:

  Every node will periodically broadcast hello messages to its neighbors. A hello message mainly maintains one-hop's local connectivity. When a node receives a hello message from another node, it means the two nodes are in the achieving range of each other. We can also get information about the joining of new nodes by receiving their hello massages.

2.3 Hybrid Routing Protocols

Obviously, proactive and reactive routing protocols have their individual advantages in different Ad Hoc network environments. Therefore, a lot of scholars have proposed hybrid routing protocol combined with both the advantages of proactive and reactive routing protocols, such as ZRP (Zone Routing Protocol) [1].

Table 1. AD Hoc Routing Protocol Classification [6]

Proactive routing	Reactive routing	Hybrid routing
DSDV, WRP, OLSR, GSR, FSR, HSR, STAR, TBRPF CGSR,	AODV, DSR, TORA, ROAM LMR, ABR, RDMAR, LAR, ARA, CBRP	ZRP, ZHLS, SLURP, DST, DDR

3 Category of Attacks in Ad Hoc Networks

These Ad Hoc routing protocols in the Table 1 rarely consider about the security because they assume that the nodes are reliable in the network. However, all nodes in the network are not honest, that is, it still has some attacks in the network. Therefore, we must consider the security of Ad Hoc network. In fact, the security of Ad Hoc network is roughly divided into two parts, the routing security and data transmission security.

Because of the cooperation relationship in the Ad Hoc networks, nodes help forwarding data to each other. When discovering route, if one malicious node modifies the fields of routing packet such as destination, source or sequence number, etc., it will result in the mistake or fail of routing discovery and consume the valuable electricity and bandwidth. This is what routing security is going to solve.

After setting up the correct route, the data can be transmitted. The transmission may be in danger with wiretap or falsify. This is what data transmission security is going to solve.

To solve the secure problem in Ad Hoc networks, we mainly rely on the fact that the route is safe first. Because after setting up the correct route, we can apply the point-to-point secure protocol to protect the data transmission security. The technology can be directly applied from wired network. Therefore, we will mainly focus on the routing security and discuss with the precaution to the possible attack.

3.1 Rushing Attack

An attacker can distribute a large number route requests with increasing sequence numbers forged to appear to be from other nodes. When the actual routing request is sent out many nodes, this way suppress it as a duplicate and thereby disrupt the actual route discovery. This attack results in denial-of-service when used against AODV routing protocols [12].

3.2 Routing Disruption Attack

Under this kind of attack, a malicious node must have a fresh route to the destination node. When it receives a route request message, it does not re-broadcast this route request packets and forges a route reply message with increasing the destination sequence number, and decreases the hot count. It also modifies the source node IP address in the IP header to a non-existent IP address.

3.3 Forge Route Reply Attack

For a malicious node, it can easily forge a faked route reply message to cause route disruption in the network.

3.4 Fake Route Error Attack

Under this kind of attack, the malicious node must know certain actual and well-connected nodes. Then, he may claim that an actual and well-connected node is now unreachable by forging route error message. This route error may have a high sequence number such that nodes will not accept any opposite information. For example: as Fig. 1, the malicious node M knows an actually well connected route between node C and node E, and it must be in the transmission range of an intermediate node A, the malicious node may impersonate the intermediate node C to unicast a fake route error message. It may forge a fake route error in the follow way.

(1) Set the route's destination node as the unreachable destination IP address;
(2) Set the intermediate node's IP address as the source IP address in the IP header;
(3) Set the unreachable destination sequence number as a number greater than the destination's sequence number.

Therefore, this kind of attack will easy cause the route disruption.

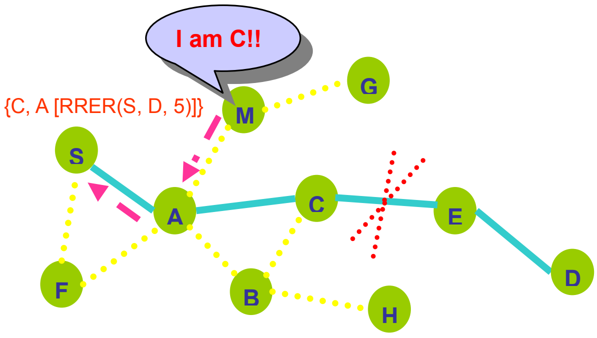
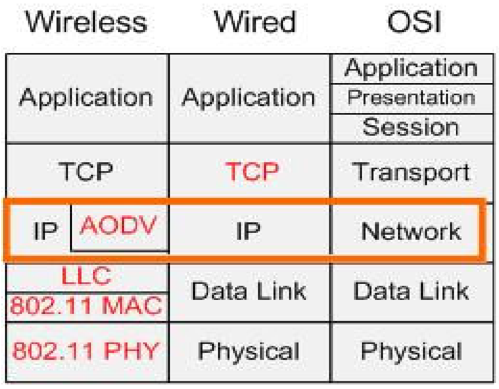


Fig. 1. Fake Route Error Attack

4 A New Routing Protocol Based on ID-MAC

Until now, many of the routing protocols (such as AODV, DSDV, DSR) suppose that nodes are honest in these routing protocols and they are able to offer safe wireless network environment. However, the network is very easy to be attacked and disrupted while there are some malicious nodes in these routing protocols.

Because Ad Hoc network is existed in an infrastructureless environment, Node is not only to regard as the terminal machine that communicates with another node but also to regard as a route helping others to convey the package. Hence, the consideration of security can be divided into two kinds: One is the security of the route protocol and the other is the security of data transmitted. Here, we just consider how to setup a secure routing protocol. The security of data transmitted is out of our study range. As Fig. 2 showed, what we want to protect is the security of the network layer and it guarantees the accuracy of the setting-up routing.



Wireless		Wired	OSI
Application		Application	Application Presentation Session
TCP		TCP	Transport
IP	AODV	IP	Network
LLC 802.11 MAC		Data Link	Data Link
802.11 PHY		Physical	Physical

Fig. 2. the Ad Hoc Wireless Stack

To avoid faked nodes and forged routing packets, we have to judge whether the route packets are modified or not. However, how to protect the part of the routing static message is shown as Fig. 3 in order to ensure integrity and non-repudiation of this part information and avoid to be forged by other nodes. The answer of this idea is signature.

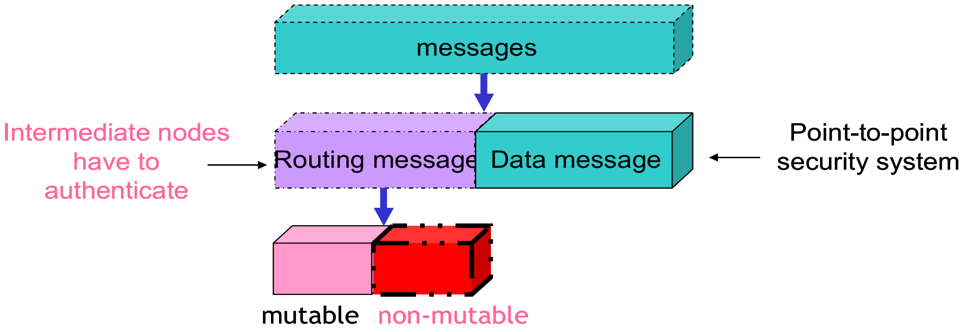

messages
Intermediate nodes have to authenticate
Routing message
Data message
Point-to-point security system
mutable
non-mutable

Fig. 3. The Protected Information

In 1984, Shamir [13] proposed a concept of identity-based cryptography. Based on this new cryptography, users' identifier information such as email or IP address instead of digital certificates can be used as public key for encryption or signature verification. In this section, we will propose a routing protocol based on ID-MAC (Identity-Based Message Access Code).

According to the definition of TESLA authentication protocol [14], [15], it needs to be loosely time synchronized between the sender and the receiver. Initially, the sender sends the key disclosure schedule by transmitting the following information to the receivers via digitally signed broadcast message. The receiver and the sender can reach each other's identity authentication.

The following parameters and notations will be used throughout this section unless otherwise specified

- K_i : Previously disclosed key.
- D_{ID_S} : The sender's ID and Q_{ID_D} is the sender's public key.
- $K_{SD} = \hat{e}(D_{ID_S}, Q_{ID_D})$: is the section key between sender and receiver.
- $H_{K_{SD}}(*)$: the hash function.

Here, there are two major procedures of this proposed scheme, Routing discovery phase and Routing maintain phase, respectively.

(1) In Routing discovery:
It assumes that five users (sender, user A, user B, user C and destination user) in this scheme. Initially, the source node S calculates two keys: the $K_{SD} = \hat{e}(D_{ID_S}, Q_{ID_D})$ is used to authenticate the legal destination node D, i.e., just only the destination node D can calculate the section key with his secret and the source node's ID to verify $K_{SD} = \hat{e}(D_{ID_D}, Q_{ID_S})$; the other key is the TESLA key ${}_{S\_}K_i$ which is used to do broadcast authentication. The following steps used to explain the routing discovery:

Step 1. Sender --> * : $\{m, H_{K_{SD}}(m), H_{S-K_i}(m \| H_{K_{SD}}(m)),$ S-$K_{i-d}\}$

Step 2. Intermediate node A: Checks the $H_{S-K_i}(m \| H_{K_{SD}}(m))$ and then computes $H_{A-K_i}(m \| H_{K_{SD}}(m))$.

Node A --> * : $\{m, H_{K_{SD}}(m), H_{A-K_i}(m \| H_{K_{SD}}(m)),$ A-$K_{i-d}\}$

Step 3. Intermediate node B: Checks the $H_{A-K_i}(m \| H_{K_{SD}}(m))$ and then calculates $H_{B-K_i}(m \| H_{K_{SD}}(m))$.

Node B --> * : $\{m, H_{K_{SD}}(m), H_{B-K_i}(m \| H_{K_{SD}}(m)),$ B-$K_{i-d}\}$

Step 4. Intermediate node C: Checks the $H_{B-K_i}(m \| H_{K_{SD}}(m))$ and then calculates $H_{C-K_i}(m \| H_{K_{SD}}(m))$.

Node C --> * : $\{m, H_{K_{SD}}(m), H_{C-K_i}(m \| H_{K_{SD}}(m)),$ C-$K_{i-d}\}$

Step 5. Destination node D : Verifies $H_{C-K_i}(m \| H_{K_{SD}}(m))$ and checks $H_{K_{DS}}(m)\ ? = H_{K_{SD}}(m)$. Then he calculates $K_{DC} = \hat{e}(Q_{ID_C}, \mathrm{D}_{\mathrm{ID_D}}) = \hat{e}(D_{ID_C}, Q_{ID_D}) = K_{CD}$ and $H_{K_{DC}}(\beta \| H_{K_{DS}}(\beta))$ where routing reply message RREP is β...

Node D --> Node C : $\{\beta, H_{K_{DS}}(\beta), H_{K_{DC}}(\beta \| H_{K_{DS}}(\beta))\}$

Step 6. Intermediate node C: Whether is $H_{K_{CD}}(\beta \| H_{K_{DS}}(\beta))$ equal to $H_{K_{DC}}(\beta \| H_{K_{DS}}(\beta))$ or not ? Then, he calculates $K_{CB} = \hat{e}(Q_{ID_B}, \mathrm{D}_{\mathrm{ID_C}})$ and $H_{K_{CB}}(\beta \| H_{K_{DS}}(\beta))$.

Node C --> Node B: $\{\beta, H_{K_{DS}}(\beta), H_{K_{CB}}(\beta \| H_{K_{DS}}(\beta))\}$

Step 7. Intermediate node B: Whether is $H_{K_{BC}}(\beta \| H_{K_{DS}}(\beta))$ equal to $H_{K_{CB}}(\beta \| H_{K_{DS}}(\beta))$ or not? Then, he calculates $K_{BA} = \hat{e}(Q_{ID_A}, \mathrm{D}_{\mathrm{ID_B}})$ and $H_{K_{BA}}(\beta \| H_{K_{DS}}(\beta))$.

Node B --> Node A: $\{\beta, H_{K_{DS}}(\beta), H_{K_{BA}}(\beta \| H_{K_{DS}}(\beta))\}$

Step 8. Intermediate node A: Whether is $H_{K_{AB}}(\beta \| H_{K_{DS}}(\beta))$ equal to $H_{K_{BA}}(\beta \| H_{K_{DS}}(\beta))$ or not? Then, he calculates $K_{AS} = \hat{e}(Q_{ID_S}, \mathrm{D}_{\mathrm{ID_A}})$ and $H_{K_{AS}}(\beta \| H_{K_{DS}}(\beta))$.

Node A --> Source Node S: $\{\beta, H_{K_{DS}}(\beta), H_{K_{AS}}(\beta \| H_{K_{DS}}(\beta))\}$.

Step 9. Source Node S : Verifies $H_{K_{AS}}(\beta \| H_{K_{DS}}(\beta))$ and checks the following equation If the Eqn. (1) exacts, then S can transmit data to node D by this routing. Otherwise, S must give up this routing and restart to broadcast RREQ message to other nodes.

$$H_{K_{SD}}(\beta) \overset{?}{=} H_{K_{DS}}(\beta) \qquad \textbf{(1)}$$

(2) In Routing Maintain:

In order to let neighbor nodes know this node still alive, nodes will broadcast hello message periodically in routing maintain. The identity authentication becomes very important. Initially, in the loosely time synchronized course with the sender; the sender sends the key disclosure schedule to the receivers via digital signature. After loosely time synchronized course, the receiver and the sender can authenticate the identity each other. Nodes broadcast hello message and use TESLA broadcast authentication to confirm that the node has not been left yet, and not be masked by the malicious node in the course of transmitting data.

5 Security Analysis

Here, we discuss the security of proposed scheme whether it reaches our required security demand which have been discussed in Sec. 3 or not.

5.1 Resist rushing attack:

The attacker used to modify original routing request packets or forge routing request packets and then broadcast them to generate the rushing attack, i.e., this attack model makes the original legal routing request packet suppressed and causes the route unable to set up. However, we use the TESLA broadcast authentication scheme to confirm the integrity of transmission message in our scheme. Therefore, any middle node can not modify or forge the transmission message unless the destination node can verify this message. Moreover, we can detect the malicious node when this attack is happened.

5.2 Resist routing disruption attack:

We assume that the malicious node can arbitrarily add the sequence with a large numbers or modify the IP header with a non-existent source node IP Address in this attack. It will make upstream node sets up wrong forward route and then causes this route is unable to be set up. However, we use TESLA broadcast authentication to confirm the legal node which has the key of the HMAC even though the malicious node modified the IP header with a non- existent source node or other node. So, it can easy detect this attack by using to verify the TESLA HMAC.

5.3 Resist forge route reply attack:

For a malicious node, this kind of attack is very easy. He can mask a node to forge a faked route reply message to cause route disruption in the network or declare that he has a route to node D and convey a forged reply. Unfortunately, the source node does not know his data has never been conveyed to node D. However, if the middle node announces he has a route to node D in our scheme, he must send notice to node D, and then the node D will send the nonce and the nonce HMAC with pairing key K_{SD}. Obviously, we can resist this attack efficiently by using to check the nonce D and HMAC with key K_{SD} in the middle node.

5.4 Resist fake route error attack:

Under this kind of attack, a malicious node must know certain actually well connected nodes. A malicious node may claims that an actually well connected node is now unreachable by forging route error message, and cause routing disruption. In proposed scheme, we use TESLA broadcast authentication to detect the fake node, and drop the forged packets. Hence, this attack can not be successful to attack our proposed scheme.

6 Simulation and Result

The simulations were conducted on Intel Pentium 4 processor at 2.4 GHz, 736 MB of RAM running on Windows XP + Cygwin + NS-2.28 + AODV. Cygwin is a suit of software that simulates Linux operating system environment. Network Simulator 2 (NS2) [16] is developed by the Lawrence Berkeley National Laboratory (LBNL). It is a suit of software that is used to analyze the efficiency of network simulation such as TCP or UDP.

6.1 Scenarios

We simulate how great the influence degree to Ad Hoc network of different attacks is, and the results show that these attacks will cause the network to be disrupted.

Scenario 1 – Rushing Attack

We discuss how great the influence degree of Ad Hoc network with rushing attack. According to section 3.1, we assume that while malicious node receives a route request packet, he increases the sequence number by at least one, and increases the broadcast ID by at least one, and then rebroadcasts route request packet. We modify the original AODV code and enable becoming malicious AODV code that does not observe the legal rule. Then the studied scenario is consisted of two kinds of network situations. The parameters are showed in Table 2 and 3, respectively. The network situation 1 is generated by ours, in order to master correct route where the package conveys. The network situation 2 is generated randomly by computer, and is used for supposing it is in the general environment. The results are showed in Fig. 4 and 5 where PDR (Packet Delivery Ratio) acts as the index of assessing the influence on whole network.

The formula of PDR is equal to $\sum \frac{CBR\ packets\ received \text{ by } CBR \text{ sinks}}{CBR\ packets\ sent \text{ by } CBR \text{ source}}$.

Table 2 Network Situation 1 Parameters

Number of nodes	30
Transmission range	250 m
Dimensions of space	750 m x 750 m
Simulation duration	300 seconds
Physical / MAC layer	IEEE 802.11 at 2 Mbps
(Min, Max) speed	1 m/s
Pause time	100sec
Malicious nodes	1, 3, 5, 7, 10, 15
Source data pattern (CBR)	4 packets/second, 512 bytes/packet
Source nodes	10

Table 3 Network Situation 2 Parameters

Number of nodes	50
Transmission range	250 m
Dimensions of space	1000 m x 1000 m
Simulation duration	300 seconds
Physical / MAC layer	IEEE 802.11 at 2 Mbps
(Min, Max) speed	20 m/s
Pause time	10sec
Malicious nodes	1, 3, 5, 7, 10, 15
Source data pattern (CBR)	4 packets/second, 512 bytes/packet
Source nodes	16

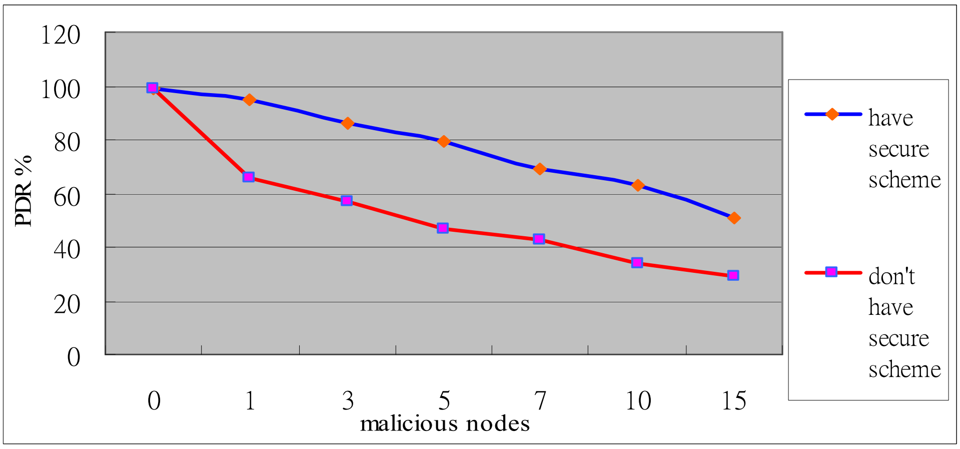


Fig. 4. The Result of 30 Nodes with the secure scheme—Rushing Attack

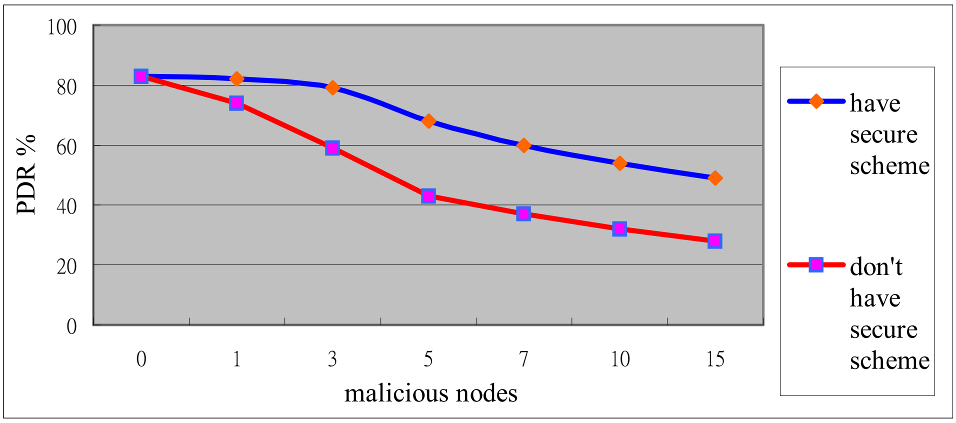


Fig. 5. The Result of 50 Nodes with the secure scheme—Rushing Attack

Scenario 2 - Modifying IP Header Attack

Similarly, we discuss how great the influence degree of Ad Hoc network with modifying IP Header attack. According to section 3.2, we also rewrite the AODV code and enable becoming malicious AODV code. The environment parameters are the same. In theory, this attack will cause great influence results. The results are showed in Fig. 6 and 7, respectively.

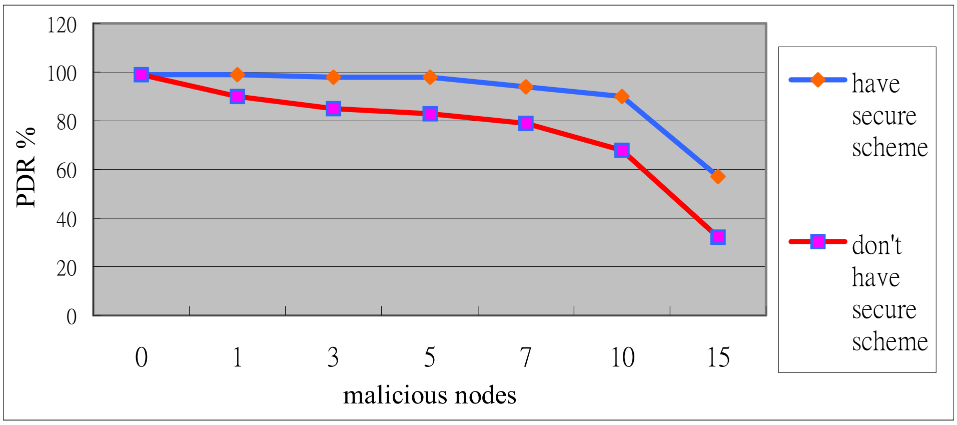


Fig. 6. The Result of 30 Nodes —forge route reply

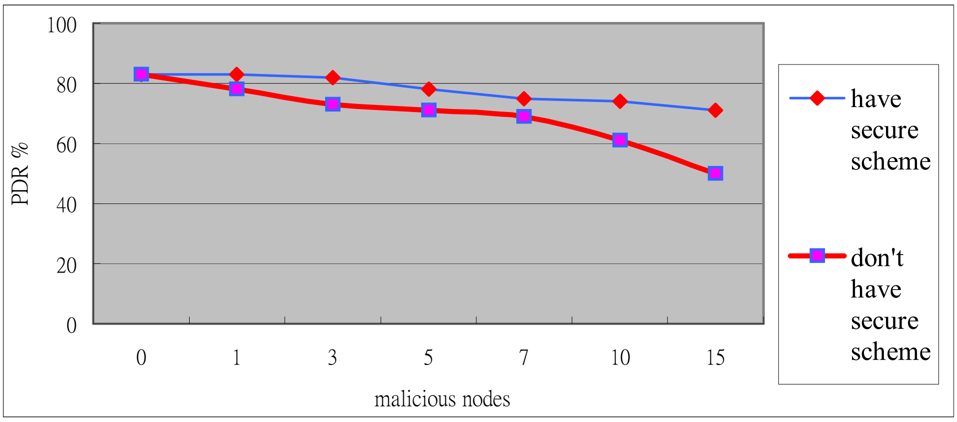


Fig. 7. The Result of 50 Nodes — forge route reply

7 Conclusions

In this paper, we propose a new secure routing protocol based on ID-HMAC. After our analysis, this scheme can not only prevent the malicious attacks such as rushing attack, routing disruption attack, forge route reply attack and fake route error attack in Ad-Hoc network but also we use NS2 to simulate these scenarios of attacks and discuss how well the efficiency is from the simulation results.

Acknowledgement

This work was supported in part by TWISC@NCKU, National Science Council under the Grants NSC 94-3114-P-006-001-Y.

References

[1] Z.J. Hass and M.R. Pearlman, “The Performance of Query Control Schemes for the Zone Routing Protocol”, IEEE/ACM Transactions on Networking, Vol. 9, No.4, pp.427-438, August 2001.

[2] D. Johnson, D. Maltz, and J. Jetcheva, “The dynamic source routing protocol for mobile ad hoc networks,” http://www.cs.cmu.edu/~dmaltz/internet-drafts/draft-ietf-manet-dsr-09.txt, July 19, 2004.

[3] J. Jubin and J. D. Tornow. “The DARPA packet radio network protocols,” Proceedings of the IEEE, Vol. 75, pp.21-32, 1987.

[4] P. Ning and K. Sun, “How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols,” Proceedings of the 4th Annual IEEE Information Assurance Workshop, pp. 60-67, June 2003.

[5] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers,” ACM SIGCOMM’94, 1994.

[6] E. M. Royer and C. K. Toh. “A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks,” IEEE Personal Communications Magazine, April 1999.

[7] B. Dahill, K. Sanzgiri, B. N. Levine, C. Shields, and E. Royer, “A Secure Routing Protocol for Ad Hoc Networks,” in Proceeding of 10th IEEE International Conference on Network Protocols (ICNP 2002), pp. 78-87, Nov. 2002.

[8] Y. C. Hu, D. B. Johnson, and A. Perrig., “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, June 2002.

[9] Y. C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks,” in Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pp. 12-23, Sep. 2002.

[10] P. Papadimitratos and Z. J. Haas, “Secure message transmission in mobile ad hoc networks,” Ad Hoc Networks Journal, Vol. 1, No.1, pp.193-209, 2003.

[11] M. G. Zapata and N. Asokan, “Securing Ad hoc Routing Protocols,” in Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), pp. 1-10, Sep. 2002.

[12] Y. C. Hu, A. Perrig, and D. B. Johnson, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,” WiSe 2003, San Diego, California, USA, Sep. 19, 2003,.

[13] A. Shamir, “Identity-based cryptosystems and signature schemes,” Crypto '84, 1984.

[14] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, “Efficient and Secure Source Authentication for Multicast,” in Network

and Distributed System Security Symposium, NDSS ’01, pp. 35–46, Feb. 2001.

[15] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," RSA CryptoBytes, 2002.

[16] http://140.116.72.80/~smallko/ns2/ns2.htm.

[17] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks”, Elsevier Ad Hoc Networks Journal, Vol. 2, No. 1, pp. 1-22, Jan. 2004.

[18] J. Cha and J. Cheon, “An Identity-Based Signature from Diffie-Hellman Groups,” Public Key Cryptography – Proceedings of PKC 2003, LNCS 2567, pp. 18-30, Springer-Verlag, 2003.

[19] W. Diffie and M.E. Hellman, “New Directions in Cryptography,” IEEE Trans. on Information Theory, Vol. IT-22, pp. 644-654, 1976.

[20] L.C Guillou, J. J. Quisquator, “A paradoxical identity-based signature scheme resulting from zero-knowledge,” CRYPTO’88 LNCS-403, pp.216-231, Springer-Verlag, 1988.

[21] J. M. Hou, A Study of Securing Ad Hoc Network: Dynamic Routing Information Protection, Master Thesis, National Cheng Kung University, Tainan, Taiwan, R.O.C. , June 2005.

[22] B Ljubica, B Levente, and C Srdjan,. “Self-organization in mobile Ad hoc,” IEEE Communications Magazine, June 2001.

[23] V. D. Parka and M.S. Corsonb, “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks,” IEEE INFOCOM, 1997.

[24] R.L. Rivest, A. Shamir, and L.M Adleman. “A method for obtaining digital signatures and public-key cryptosystems,” Communication of the ACM, Vol.22, pp.120-126, 1978.

[25] L Subramanian, H Randy. “An Architecture for Building Self-Configurable Systems,” IEEE Workshop on Mobile Ad Hoc Networking and Computing. Boston, Aug. 2000.

[26] S Yi, P. Naldurg, and R. Kravets, Security-aware Ad-Hoc routing for wireless networks, Tech Rep: UIUCDCS-R-2001-2241, Department of Computer Science, University of Illinois at Urbana-Champaign, Aug. 2001.

[27] J. Zhen and S. Srinivas “Preventing Replay Attacks for Secure Routing in Ad Hoc Networks Proc,” the Second International Conference on Ad Hoc, Mobile and Wireless Networks, Montreal, Canada, Oct. 8-10, 2003.