Advanced Science and Technology Letters
Vol.134 (CIA 2016), pp.16-20
http://dx.doi.org/10.14257/astl.2016.134.03

An Authentication Scheme of Ad-Hoc Network against the Attacks

Haiyan Liu[1], Kongjun Bao[1],

[1] Engineering Training Center, Zhengzhou University of Light Industry,
450002 Zhengzhou, China
{2003056, baokongjun}@ zzuli.edu.cn

Abstract. In this paper, some typical wireless attacks are considered, such as masquerade attack, black hole attack and replay attacks. To against the attacks which threat seriously security of Ad Hoc network, a new authentication scheme is proposed. The proposed scheme involves three main stages. Some advantages and drawbacks are discussed compared with other solutions presented in previous researches.

Keywords: Ad-Hoc network, black hole attack, masquerade attack, authentication

1 Introduction

Ad Hoc network is a multi-hop temporary communication network of mobile nodes equipped with wireless transmitters and receivers without the aid of any current network infrastructure. [1] Due to lack of infrastructure support in Ad Hoc network, such network is more available. Security in mobile ad hoc networks is difficult to achieve.

Ad Hoc network possesses some traits: the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, the absence of a certification authority, and the lack of a centralized monitoring or management point. The flexibility of Ad Hoc Network brings the significant challenges in security. A new authentication solution is presented in this paper. The proposed scheme involves three main stages: intermediate nodes pre-authenticating stage, common key k_i between n_0 and n_i negotiating stage and authentication during all routing phases.

2 New scheme against typical attacks

In this section, we propose an authentication scheme which can greatly mitigate the typical attacks, which includes simple black hole attacks and cooperative attacks. The solution focuses on authentication techniques during all routing phases, i.e, all the nodes involved routing path must be authenticated through the proposed authentication scheme before participating in communicating with other nodes. Our

ISSN: 2287-1233 ASTL

solution utilizes authentication method to exclude attackers and unauthorized nodes from participating in the routing. The solution consists of three stages and relies on a certificate authority (CA).

2.1 Some assumptions and definitions

The proposed scheme is implemented based on some assumptions and definitions which are as follows.

1. It is assumed that a certificate authority is available. As we known, the lack of any fixed central infrastructure or administration leads to that key management is problematic in MANETs. But many solutions have been presented previously, such as the key distribution protocols in [2] which put forward private key management protocols, distributed fully key management solution presented by Capkun. This problem is not discussed in this paper.
2. Key pair (p_{kni} ,kpri)between n_i and CA have been existed, which is generated in the procedure of n_i entering Ad Hoc Network .This procedure is not discussed in this paper.
3. Secure channel between CA and each nodes is existent.
4. The number of the communication route from source node n_0 to destination node n_{m-1} is denoted by m, where n_i (i=0,1,2,3,…,m-1)represent the set of nodes constituting the routing path.
5. The private key of each node in the routing path is denoted by S_i(i=0,1,2,3,…,m-1).
6. Each node's identity is denoted by ID_i which is stored in a table of CA.
7. It is assumed that wireless links are bidirectional, because our solution requires a bidirectional exchange of packets.
8. The source node n_0 and the destination node n_{m-1} are trustworthy, i.e., at least the source node and the destination node does not disclose in any case its shared key.

2.2 The proposed scheme

Based on assumptions mentioned above, the proposed new scheme consists of three main stages: intermediate nodes pre-authenticating stage, common key k_i between n_0 and n_i negotiating stage and authentication during all routing phases stage. New scheme is illustrated in Fig.1.

As shown in Fig.1, in the stage 1 each node n_i(i=1,2…m-2) from source to destination in the routing path must propose authentication request packet to the source node n_0, n_0 extract some useful information from the request packet and then transmit it to the CA, details will be discussed later.CA receives the request packet and delivers the authentication result to the n_0 after processing.n_0 records the result attached n_i. It is noted that the procedure of n_i authentication to n_0 is rational, because the node in Ad Hoc Network contains AP functionality as we known. Here n_0 acts as AP in the pre-authentication.

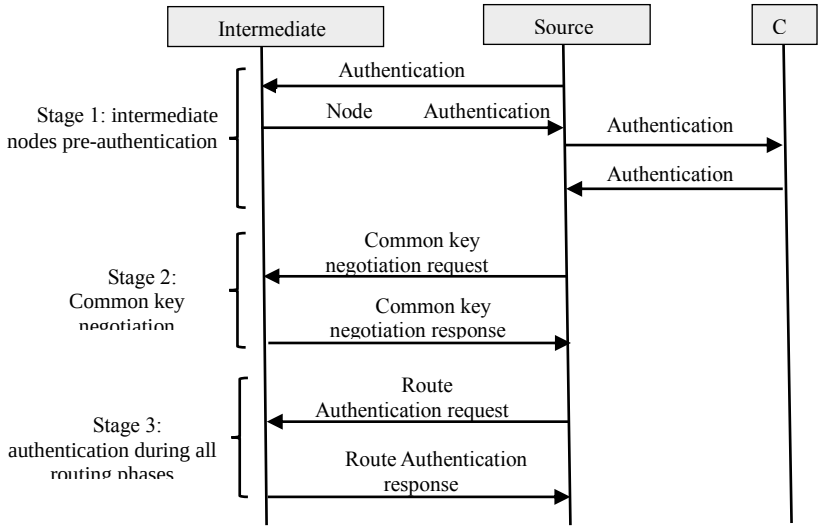

Fig. 1. Three stages of the scheme

The common key k_i(i=1,2…m-2) between source node n_0 and intermediate node n_i is generated in stage 2. In the stage above, the n_0 receives the authentication response message from CA. In this stage n_0 will decide whether calculates the common key or discard message according to the authentication result. If CA authenticates n_i successfully, n_0 will calculate the common key k_i based on the information contained in the message and then return the corresponding calculated response message to the n_0, The computed common key k_i is used for the following route authentication in the next stage.

The most important authentication procedure of all is in the third stage. In this stage, n_0 will send the route authentication request message involved some encrypted message and other processed information to the n_i. The n_i receives the message, and then return it to the n_0 after necessary processing. The n_0 make a judgment whether the n_i is a malicious node by analyzing the corresponding information in the response message. If n_i is suspected to be a malicious node, the current routing path will be considered as insecure. Source node n_0 will abandon this route and seek another route again to avoid the black hole node.

3 Simulation and analysis

The simulation of proposed scheme is presented in this section. The Delivery ratio is the main metric we considered.

The simulator which we conducted our solution making use of is the network simulator (ns-2.35) [3] . In the hypothetical network, 50 wireless mobile nodes move

randomly in a square area with the size of 1000 meter. Nodes' movement and position according to the random waypoint model. The related simulation parameters are shown in Table 1.

Table 1. Parameters in Simulation

Parameters	**Values**
Simulation area	1000*1000
mobility model	random way point
Link Layer type	LL
Protocols studied	AODV/DSR
Simulation time	100 sec
Maximum speed	20m/s
Maximum Pause time	5 sec
Traffic type	CBR(UDP)
CBR rate	50 Kbps
Number of nodes	30
Number of Malicious Nodes	2
Hash function	SHA-1

Delivery ratio is the ration of the packets received by the destination node to those generated by the CBR sources. As shown in Fig.2, the delivery ratio significantly reduces both in AODV-based network and DSR-based network under black hole attacks without scheme. The simulation results indicate that the proposed authentication scheme is efficient against attacks.

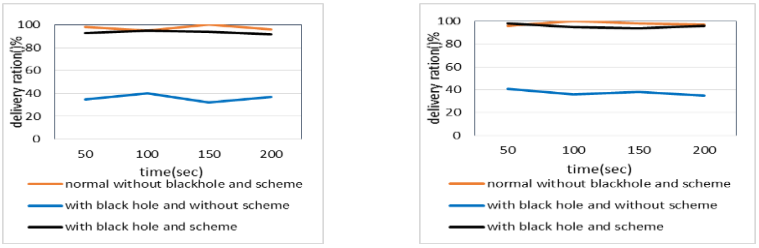

Fig. 2. Delivery ration

4 Conclusion

The authentication scheme proposed in this paper composed by three stages. The simulation results indicate that the delivery ratio and end to end delay of proposed solution is similar to the network without attacks. In summary, the proposed scheme is efficient and practical to against attacks.

References

1. Nakayama, H., Nemoto, Y., Kato, N.: A Survey of Routing Attacks in Mobile Ad Hoc Networks, IEEE Wireless Communications, (2007)
2. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. LNCS, vol. 3287, pp.293--315 (2003)
3. Mohanapriya, M., Krishnamurthi, I.: Modified DSR protocol for detection and removal of selective black hole attack in MANET, Computers and Electrical Engineering, vol. 40, pp. 530--538 (2014)