Poster: Secure Routing with Tamper Resistant Module for Mobile Ad Hoc Networks

Joo-Han Song, Vincent Wong and Victor Leung
Department of Electrical and Computer Engineering
The University of British Columbia
2356 Main Mall, Vancouver, BC, Canada V6T 1Z4
e-mail: {joohans, vincentw, vleung}@ece.ubc.ca

Yoji Kawamoto
Network and Software Technology Centre
Sony Corporation
6-7-35 Kitashinagawa Shinagawa-ku, Tokyo, Japan
e-mail: kawamoto@sm.sony.co.jp

1. INTRODUCTION

Most routing protocols proposed for mobile ad hoc networks (MANETs) assume that there is an implicit *trust-your-neighbor* relationship in which all the neighboring nodes behave properly. However, we should not ignore the fact that attackers do exist in real networks. These users may try to paralyze the MANETs by manipulating the messages (e.g., dropping all data or control packets, sending incorrect route advertisement messages). Thus, secure routing protocols are crucial for MANETs.

There are a number of secure ad hoc routing protocols proposed in the literature with the aim of preventing either message tampering or dropping attacks [1, 2]. However, these protocols do not consider the possibility of routing module tampering attack by either malicious or compromised users. In addition, some of the secure routing protocols assume that there is either *a priori* trust between network entities or a centralized online trusted server in the network [2].

Since routing functionalities are usually implemented in software, it is possible for an attacker to alter the content of the routing table in a mobile device. For example, an attacker can create a routing loop by changing the routing entries in the routing table. Packets may be forwarded to an incorrect neighboring node and never reach their intended destination. Such attacks are difficult to detect, and may disable the network even though routing messages are fully protected by previously proposed security mechanisms. Thus, it is important to develop mechanisms that protect the routing module from both malicious and compromised users. To address this important problem in routing security, we propose the use of a Tamper Resistant Module (TRM) to protect the routing module. From a security point of view, we define the TRM as a hardware/software entity in which data and program cannot be modified by the user. Thus, routing module tampering attacks can be prevented.

Assuming that each mobile node incorporates a TRM that performs the routing and Medium Access Control (MAC) functions, we propose a secure routing mechanism for the Ad hoc On-demand Distance Vector (AODV) routing protocol [3]. The Secure AODV (SAODV) routing protocol can prevent routing message tampering attacks without either *a priori* trust between network entities or a centralized online trusted server. Moreover, we propose a Secure Data Forwarding (SDF) mechanism to combat black hole attacks.

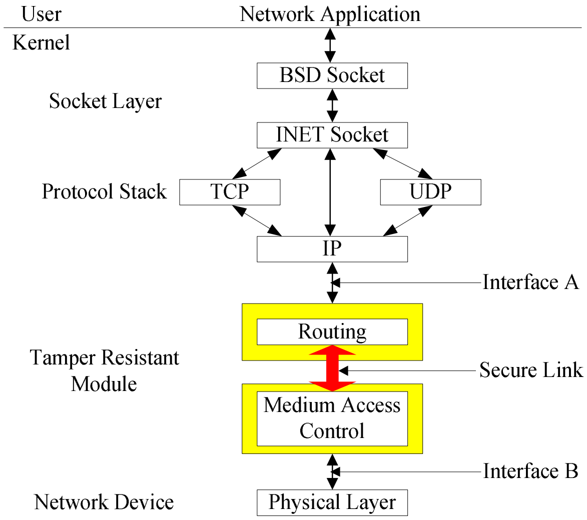


Figure 1. Tamper Resistant Module in Linux

2. SECURITY MECHANISMS

In this section, we first describe the functionalities of the proposed Tamper Resistant Module (TRM). We then describe our proposed SAODV routing protocol and the corresponding SDF mechanisms.

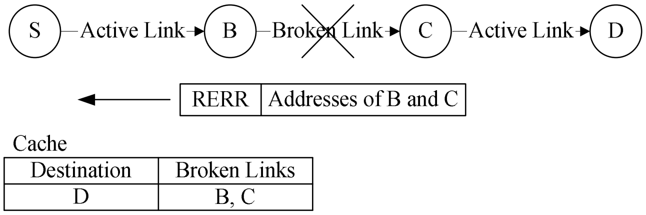
2.1 Tamper Resistant Module (TRM)

We propose the use of TRM to protect both the routing module and the MAC layer. By including the MAC layer within the TRM and employing the SDF mechanisms, data integrity can also be maintained.

The routing module is typically implemented in software while the MAC layer functionalities are implemented in hardware/firmware (e.g., network interface card). A natural question is how to implement the TRM in a mobile node (e.g., notebook computer). To this end, we propose the use of tamper resistant hardware [4] for the MAC layer and the use of tamper resistant software [5] for the routing module. We assume that there is a secure connection between the routing module and the MAC layer.

Figure 1 shows the reference design of using the TRM in the Linux-based mobile node [6]. We assume that all the secret information, such as the asymmetric keys, is stored in the TRM.

MobiHoc'03, June 1-3, 2003, Annapolis, Maryland, USA.
Copyright 2003 ACM 1-58113-684-6/03/0006…$5.00.



Destination	Broken Links
D	B, C

Figure 2. Example for Black Hole Attack Prevention

2.2 Secure AODV Routing Protocol

We propose the use of the double signature for the RREQ (Route Request) and RREP (Route Reply) packets for message authentication and integrity. In each routing packet, the digital signature is applied twice, the first time for the non-mutable part and the second time for the mutable part. The drawback of double signature is the increase in computational complexity when compared with the shared secret key method. To this end, we suggest the use of Elliptic Curve Cryptography (ECC) [7] instead of RSA.

To implement the SAODV routing protocol, we assume that all mobile nodes deploy the TRM, and the Certification Authority (CA) only issues a certificate to the authorized TRM-based mobile nodes. We do not assume that the participating nodes in the MANET have the same common shared key in advance because this may not be feasible in practice.

To prevent the black hole attack for data packets, we propose an extension of the AODV RERR (Route Error) packet to include the addresses of the two end nodes of the broken link. The source node will append those two addresses in the RREQ packet for route discovery. The new route will not include the two end nodes of the broken link (see Figure 2).

Note that since the TRM does not allow the users to send consecutive intentional RREQ packets to the network if there is a corresponding route entry in its routing table, the intensity of the DoS (Denial of Service) attack can be reduced in the network layer.

2.3 Secure Data Packet Forwarding (SDF)

We also propose a security mechanism for data packet forwarding. To achieve this, each node in the route needs to check the integrity of the data packets. Note that the use of digital signatures in data packets may not be suitable due to the high computation power required to generate and verify the digital signature of each data packet. In our proposed mechanism, we use a symmetric method such as HMAC [8], which is a Message Authentication Code mechanism for message authentication using cryptographic hash functions based on a secret key. For the symmetric method, we need to determine when and how each node exchanges the shared secret key with its neighbors. Since each participating node of the route has to exchange RREQ and RREP packets during the route discovery phase, we propose the use of the Elliptic Curve Diffie-Hellman (ECDH) [9] method to generate the symmetric keys for the HMAC.

3. PERFORMANCE EVALUATION

We perform simulation experiments to evaluate the performance of the proposed TRM-based SAODV, with and without SDF, in the presence of black hole attackers, using ns2 version b8a [10]. Since mobile nodes use TRMs to protect the routing and MAC modules, TRM-SAODV with SDF can detect the black hole attack. However, for TRM-SAODV without SDF, the black hole attacker can drop the data packets and forge the link layer ACK (acknowledgement) to its neighboring node. In that case, the network is unable to detect the presence of black hole attackers.

Simulation results showed that in the presence of black hole attackers, the proposed mechanisms increase the packet delivery fraction at the expense of a higher average end-to-end delay and routing overhead.

4. CONCLUSIONS

In this study, we have proposed techniques to improve the security of ad hoc routing protocols. First, we have proposed the use of TRMs to prevent routing module tampering attacks by malicious or compromised users. Such attacks are hard to detect, and cannot be prevented by existing secure routing protocols. We have proposed a secure routing mechanism for the AODV routing protocol that uses double signatures in both RREQ and RREP packets to prevent routing message tampering attacks, and broken-link information in RREQ and RERR packets to prevent black hole attacks. For secure data transmission, we have proposed the use of HMAC to maintain the message integrity and prevent data message replay attacks. The ECDH method is used to generate the symmetric keys for HMAC.

Further simulation experiments are in progress to compare the performance between different secure routing protocols. We are also studying the implementation issues of our proposed TRM in the routing module and MAC module.

5. REFERENCES

[1] H. Yang, X. Meng, and S. Lu, "Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," in *Proc. of ACM WiSe'02*, Atlanta, Georgia, Sept. 2002.

[2] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," in *Proc. of ACM MobiCom'02*, Atlanta, Georgia, Sept. 2002.

[3] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," *IETF Internet Draft*, February 2003.

[4] O. Kommerling and M. G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," in *Proc. of USENIX Workshop on Smartcard Technology*, Chicago, 1999.

[5] D. Aucsmith and Graunk, "Tamper Resistant Software: An Implementation," in *Proc. 1st International Workshop on Information Hiding*, Springer Lecture Notes, 1986.

[6] D. Rusling, "The Linux Kernel," http://www.tldp.org/LDP/tlk/tlk.html

[7] D. Johnson, "ECC, Future Resiliency and High Security Systems," *Certicom White Paper*, March 1999.

[8] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," *IETF RFC 2104,* Feb. 1997.

[9] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. on Information Theory*, 1976.

[10] The Network Simulator - NS-2 Notes and Documentation and Source Code.