Secure Ad hoc On-Demand Distance Vector Routing

Manel Guerrero Zapata
manel.guerrero-zapata@nokia.com
Mobile Networks Laboratory
Nokia Research Center
FIN-00045 NOKIA GROUP, Finland

This article gives an overview of different approaches to provide security features to routing protocols in mobile ad hoc networks (MANET). It also looks to Secure AODV (an extension to AODV that provides security features) giving a summary of its operation and talking about future enhancements to the protocol.

I. Introduction

Mobile ad hoc networks (MANET) protocols are being designed without having security in mind. In most of their specifications it is assumed that all the nodes in the network are friendly. The security issue has been postponed and there used to be the common feeling that it would be possible to make those routing protocols secure by retrofitting pre-existing cryptosystems.

Nevertheless, securing network transmissions without securing the routing protocols is not sufficient. Moreover, by retrofitting cryptosystems (like IPSec [KA98]) security is not necessarily achieved.

Therefore, in manet networks with security needs, there must be two security systems: one to protect the data transmission and one to make the routing protocol secure. There are already well studied point to point security systems that can be used for protecting network transmissions. But there is no much work about how make manet routing protocols discover routes in a secure manner [ZH99, JC99].

II. Symmetric vs. Asymmetric Cryptography

If in a MANET network all routing messages are encrypted with a symmetric cryptosystem, it means that everybody that we want to be able to participate in the network has to know the key. That is not a big problem if we are a "team" of persons that meet to let every member of the team to know the "team-key" and then we go to play on the ground creating a MANET network. A member of the team trust the other members of the team, so they assume that a member of the team will not do anything nasty to the other members. They trust and authorize the other members to change their routing tables.

Maybe this is the best thing to do for military scenarios (besides the problem of the compromised nodes and some others).

But now, let's thing that we want to create a MANET network where everybody can participate. Maybe in a convention, in a meeting room, in a campus, or in our neighborhood. Then we have a problem, we do not trust the others. We are not a team. So what do we do now? How do we force everybody to be honest? Maybe what we can do is to only believe a routing information if the originator of such information is the destination of the route (in such a way that if you lie (since you can only lie about yourself) the only benefit you get is that people is not able to communicate with you.

With this scenario in mind, the best option would be to use an asymmetric cryptosystem (with public an private key pairs) so that the originator of the route messages signs the message. It would not be needed to encrypt the routing messages because they are not secret. The only requirement is that the nodes will be able to detect forged routing messages.

III. Misbehaving Detection Schemes

Some work has been done to secure ad hoc networks by using misbehavior detection schemes (e.g., [MGLB00]). This kind of approach has two main problems:

- It is quite likely that it will be not feasible to detect several kind of misbehaving (specially because it is very hard to distinguish misbehaving from transmission failures and other kind of failures).
- It has no real means to guarantee the integrity and authentication of the routing messages.

Therefore, it is quite obvious that this approach is just not feasible. Any malicious node can generate forged misbehaving reports, making believe everybody that the rest of the nodes are even more evil that itself.

IV. Obscurity and Tamper Resistant Devices

Since there has not been, so far, a clear way to secure ad hoc networks, some people have decided to dust off the tamper resistant approaches. We will just refer to [AK96, AK97, BS97] where it is discussed why "trusting tamper resistance is problematic".

Obscurity is not the way to obtain security. There is not such a thing as a tampering resistant device. Therefore, trying to combine symmetric cryptography solutions with tamper resistant devices to create the same result provided by alternatives that use asymmetric cryptography does not make sense.

V. Secure AODV

The Secure Ad hoc On-Demand Distance Vector (SAODV) [Gue01] addresses the problem of securing a MANET network. SAODV is an extension of the AODV [PRD02] routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation.

SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node. How this is achieved is the concern of the key management scheme.

Two mechanisms are used to secure the AODV messages: digital signatures to authentify the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). This is because for the non-mutable information, authentication can be performed in a point-to-point manner, but the same kind of techniques cannot be applied to the mutable information.

Route error messages are protected in a different manner because they have a big amount of mutable information. In addition, it is not relevant which node started the route error and which nodes are just forwarding it. The only relevant information is that a neighbor node is informing to another node that it is not going to be able to route messages to certain destinations anymore.

Therefore, every node (generating or forwarding a route error message) uses digital signatures to sign the whole message and that any neighbor that receives verifies the signature.

VI. Future Work

Nowadays, I am working in a new version of SAODV. In the new version there will be some minor modifications to avoid certain possible attacks that could be performed against SAODV. In addition, some other modifications will address the need to reduce the processing power requirements of SAODV due to the use of asymmetric cryptography. This is going to be achieved by allowing nodes to forward routing messages before verifying it. In the case of a route discovery, the node will only need to verify the route request message after receiving and forwarding the corresponding route reply. This will avoid that all the nodes that will be not in the selected path will have to verify route request messages (with all the computation overhead that this requires).

Another thing I am planning to do is to add SAODV extension to the NRC-AODV (the Nokia Research Center AODV implementation for Linux created by me). NRC-AODV has most of the AODV features, and was tested in the first AODV interoperability test.

VII. Acknowledgments

N. Asokan (working in the Communication Systems Laboratory at Nokia Research Center) has contributed to SAODV with several improvements and corrections. Among other contributions, he came up with the way to authenticate the hop count in the routing messages by using hash chains.

Elizabeth M. Belding-Royer has kindly posted the SAODV draft under its AODV web page:
`http://www.cs.ucsb.edu/~eroyer/txt/saodv.txt`

References

[AK96] R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. Proceedings of the Second Usenix Workshop on Electronic Commerce, pp. 1–11, November 1996., November 1996.

[AK97] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In *IWSP: International Workshop on Security Protocols, LNCS*, 1997.

[BS97] Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In *CRYPTO*, pages 513–525, 1997.

[Gue01] Manel Guerrero. Secure ad hoc on-demand distance vector (SAODV) routing, August 2001. INTERNET-DRAFT draft-guerrero-manet-saodv-00.txt.

[JC99] S. Jacobs and M. S. Corson. Manet authentication architecture, February 1999. INTERNET-DRAFT draft-jacobs-imep-auth-arch-01.txt.

[KA98] S. Kent and R. Atkinson. Security architecture for the internet protocol. IETF Request for Comments, November 1998. `RFC 2401`.

[MGLB00] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Mobile Computing and Networking*, pages 255–265, 2000.

[PRD02] Charles E. Perkins, Elizabeth M. Royer, and Samir R. Das. Ad hoc on-demand distance vector (AODV) routing. IETF INTERNET DRAFT, MANET working group, January 2002. `draft-ietf-manet-aodv-10.txt`.

[ZH99] Lidong Zhou and Zygmunt J. Haas. Securing ad hoc networks. *IEEE Network Magazine*, 13(6), November/December 1999.