무선 Ad Hoc 환경에서의 보안 설계 분석

김정태
목원대학교

Analyses of Security Issues in Wireless Ad Hoc Communication

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

A Mobile Ad Hoc Network is a system of wireless mobiles nodes that dynamically self-organized in arbitrary and temporary network topologies allowing people and devices to inter-network without any preexisting communication infrastructure. Taking into account its nature and challenges and security issues, we present current security solution and analyse the scheme for protecting attacks.

I . Introduction

Wireless mobile multihop an hoc networks, or MANETs, are wireless networks that do not require fixed infrastructure support. Nodes play a dual role: they act as traffic sources/sinks as well as traffic forwarders. Due to mobility and the volatile nature of wireless links, MANETs may be subject to frequent topology changes. Therefor, one of the main challenges faced by MANET routing protocols is to be able to provide routes in the face of frequent topology changes.
Mission-critical operations such as military, battlefield, emergency and disaster rescue are some of the key applications of MANETs. For most of these applications, robustness and security are critical requirements. This is exacerbated in MANETs due to their "openness" since any participating node can potentially serve as traffic routers. Therefore, attacks such as interception, eavesdropping, and jamming can easily be deployed. Another challenge in providing security services in MANETs is the fact that nodes typically have limited processing, storage, power, and communication capabilities which may render some traditional security mechanism prohibitively expensive. Consequently, securing MANETs is considerably more challenging than securing wired or even "infrastructure-based wireless" networks.
MANET routing, as well as secure routing protocols assume mechani는, such as reliable data link layer and route maintenance, which were not designed for and cannot cope with malicious disruption of the data transmission. Reliable transport protocols cannot address the problem either: an attacker can forge, for example, transmission control protocol acknowledgment, while dropping data packets, misleading two communicating nodes that the data flow is undisrupted. End-to-End security such as the IP security authentication header protocol can prevent adversaries from forging or corrupting data and feedback. But IPsec does not allow the sender to detect loss of data and, thus, take any corrective action.

II. Concepts of Wireless Ad Hoc

Network

Wireless sensor networks share similarities with as-hoc wireless networks. The dominant communication method in both is multi-hop networking, but several important distinctions can be drawn between the two. Ad-hoc networks typically support routing between any pair of nodes, whereas sensor networks have a more specialized communication pattern. Most traffic in sensor networks can be classified into one of three categories:

1) Many-to-one: Multiple sensor nodes send sensor readings to a base station or aggregation point in the network.

2) One-to-many: A single node multicasts or floods a query or control information to sever sensor nodes.

3) Local communication: Neighboring nodes send localized messages to discovered and coordinate with each other. A node may broadcast messages intended to be received by all neighboring nodes or unicast messages intended for a only single neighbor.

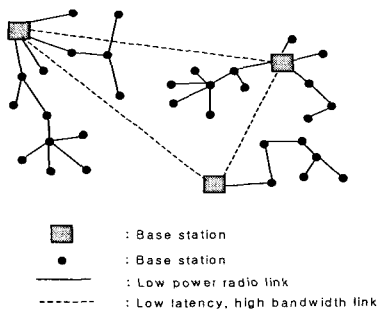

Figure 1. A representative sensor network architecture

III. Security Aware Routing Protocols

A number of security aware routing protocols currently exist that safeguard the routing operation against different kinds of attacks, denial of service, packet littering, network partitioning, etc, SEAD and ARIADNE are two secure routing protocols representitive of the two main types of routing protocols representitive of the two main types of routing classes: proactive and reactive schemes. SEAD is a proactive protocol based on DSDV that is easy to implement and efficient in terms of required memory and CPU processing capacity. It uses an efficient one-way hash function is simple to compute but infeasible to invert. SEAD is robust against uncoordinated attacks and safeguards DoS attacks. Security wise, SEAD does not provide a way to prevent an attacker from tampering with "next hop" or "destination" columns.

IV. Security Issues for Mobile Ad Hoc Networks

4.1 Secure routing

Routing of packets from a basis of the MANET where intermediate nodes route the data from the source to the destination. Assumption is that encryption keys have already been established between the communicating nodes. The efficient packets routing is one of the crucial functionalities required in an ad hoc network. It includes monitoring network traffic, prioritizing the sending of the data packets, authenticating the packets from legitimate nodes, and keeping track of updated routes. Thus, as the message is broadcasted, each node carries out above mentioned functions to thwart various attacks based on the routing protocol.

4.2. Secure data forwarding

Secure routing is the pre-requisite for implementing secure data forwarding. The motivation is to securely forward data in MANET's in the presence of malicious nodes after the route between the source and target is discovered. There are various schemes proposed for secure data

forwarding such as data forwarding based on neighbor's rating, implementing currency system in network for packet exchange, and redundantly dividing and routing message over multiple network routes.

4.3. Threshold cryptography

Threshold cryptography(TC) involves sharing of a key by multiple individuals called shareholders engaged in encryption or decryption. The objective is to have distributed architecture in a hostile environment. Other than sharing keys or working in distributed manner, TC can be implemented to redundantly split the message into n pieces such that with t or more pieces the original message can be recovered. This ensures secure message transmission between two nodes over n multiple paths. Threshold schemes generally involve key generation, encryption, share generation, share verification, and share combining algorithms. Share generation, for data confidentiality and integrity, is the basic requirement of any TC scheme.

V. Security Issues for Mobile Ad Hoc Networks

It is a popular misconception that "security" is synonymous with "encryption:, In many cases, confidentiality via encryption is that least important element of a security solution. Network security involves a number of different elements.

1. data origin authentication
2. command authorization
3. message integrity protection
4. message replay prevention
5. data confidentiality
6. key distribution
7. trust versus trustworthiness

In addition to authentication, Integrity, confidentiality, availability, access control and non-repudiation, which have to be address differently in a mobile, wireless, battery-powered and distributed environment, mobile as hoc networks raise the following security issues;

A. Cooperation and fairness

There is trade-off between good citizenship, cooperation, and resource consumption, so nodes have to economize on their resources. At the same time, however, if they do not forward messages, others might not forward either, thereby denying them services. Total non-cooperation with other nodes and only exploiting their readiness to cooperate is one of several boycotting behavior patterns. Therefore, there has to be an incentive for a node to forward messages that are not destined to itself. Attacks include incentive mechanism exploitation by message interception, copying, or forging.

B. Confidentiality of Location

In some scenarios, for instance in a military application, routing information can be equally or even more than the message content itself.

C. No traffic diversion

Routers should be advertised and set up adhering to the chosen routing protocol and should truthfully reflect the knowledge of the topology of the network. By diverting the traffic in the following ways, nodes can work against that requirement.

D. Routing

To get information necessary for successful malicious behavior, nodes can attract traffic to themselves or their colluding nodes by means of false routing advertisement. Although only suitable for devices that have enough power, a lot of information can be gathered this way by malicious nodes for later use to enable more sophisticated attacks.

E. Forwarding

Nodes can decide to forward messages to

partners in collusion for analysis, disclosure, or military benefits.

VI. Security Analyses

Attack model 1: Signaling message spoofing. Our security mechanism uses digital signature to protect the authenticity of non-mutable parameters in the sigaling messages (requested QoS by the originator or the reservation request by the destination). We also designed a lightweight hop-by-hop authentication protocol to provide authenticity to the mutable parameters of signaling messages(measurement of available resources along a candidate route). Delayed key disclosure guarantees that a malicious node is not able to forge MACs with an already released key. In our mechanism, as long as the key is not compromised, the identity of a legitimate node can not be spoofed by an attacker. In one-way hash chain authentication, we choose the function H that is simple to compute nonetheless is computationally infeasible in general to invert. Therefore, it is extremely difficult, if not impossible, to guess the key based on the already released keys.

Attack model 2: Denail of QoS request. A malicious node may intentionally drop QoS requests from a specific node in order to prohibit QoS from being available to the victim. We use "overhearing" technique in signaling messages relay, therefore an upstream node is able to listen if thenode has delivered the messages to observe the adjacent node's traffic and analyze if the drop is caused by insufficient resources or malicious intention.

Attack model 3: Malicious alteration of non-mutal parameters in transmission. By utilizing digital signature, the non-mutal parameters in QoS request or reservation messages can be effectively protected.
Attack model 4: Intentional provision of fallacious QoS states information. To thwart this type of attacks, we take advantage of the characteristics of open medium in MANETs in our intrusion detection mechnism. An upstream node can detect false QoS state information deliberately distributed by its asjacent downstream node. This hop-by-hop detection is not only able to detect attacks fast but also capable of locating the malicious node on the path, so that the malicious node can be punished or even excludes from the network to prevent further attacks.

VI. Conclusion

We have analysed design of agent for intrusion detection in wireless Ad Hoc Networks. And, we have identified some major components that contribute to the security level of MANETs. The optimum management of critical control informatin distribution is seen as the major technical goal. Critical information includes, keys and certificates, routing information, identity information and packet forwarding control information.

References

[1] V. Raghunathan, C. Schurgers, S. Park, "Energy-aware Wireless Microsensor Networks", IEEE Signal Processing Magazine, Vol. 19, N.2, IEE, March 2002, pp.40-150
[2] L. Zhou, "Securing ad hoc networks", IEEE Network Magazine, v.13, n.6, November, 1999
[3] J. Kulik, "Negotiation-based protols for disseminating information in wireless sensor networks", Wireless Network, v.8, n.2, pp.169-185,2002