유비쿼터스 환경하에서의 이동 Ad Hoc Network의 라우팅 및 정보보안 분석

김정태
목원대학교

Analyses of Routing Protocol and Security in Mobile Ad Hoc Networks in Ubiquitous Surroundings

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

요 약

본 논문에서는 이동 통신망하에서의 Ad Hoc 네트워크에서의 프로토콜을 분석 비교하고, 유비쿼터스 환경하에서의 Ad Hoc 환경하에서의 정보보안 대책을 분석하고자 한다. 이러한 분석을 통하여 차세대 멀티미디오통신하에서의 유선망과 이동망과의 정보를 교환할 대 발생할 수 있는 데이터의 정보를 보호 할 수 있는 알고리즘과 프로토콜을 제안하고 분석한다.

Ⅰ. Introduction

An ad hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to keep the network connected. Most or all nodes participate in network functions, such as routing and network management, depending on their capacity. The current trend in military ad hoc networking is to deploy technologies based on open standards that are widely used in the civilian environment, Current cryptographic solutions mainly solve security mechanism that are related to external attacks, such as protecting the communications from being eavesdropped or tampered with. These methods protect the ad hoc networks from some attacks. However, they face the following difficulties.

- The restrictions on power consumption and computation capabilities prevent the usage of complex encryption algorithms. The time synchronization cannot be efficiently achieved for hash chains.
- The constantly changing topology and dynamic membership increase the difficulty of authentication and key distribution
- Some attacks cannot be detected by the localized monitoring. Therefore, intrusion detection and intruder identification based on these methods are restricted.

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.

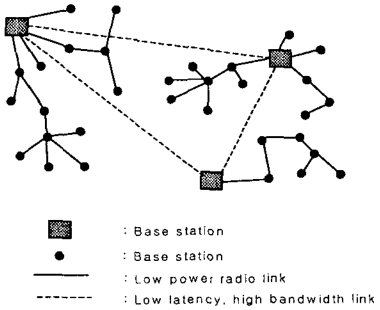
▨ : Base station
● : Base station
—— : Low power radio link
------- : Low latency, high bandwidth link

Figure 1. A representative sensor network architecture

III. A Mobile Routing Infrastructure

Each node in a mobile as hoc network logically consists of a router with possibly IP addressable hosts and multiple wireless communications devices, or may be integrated into a single device such as a laptop or handheld computer. A set of nodes making up a Magnet area is essentially a "mobile routing infrastructure" and can operate in isolation or be connected to the greater Internet via exterior routing functionality. The nodes are equipped with wireless transmitters and receivers using antennas that can be omnidirectional, highly directional, steerable, or some combination thereof. At a given point in time, depending on the nodes positions, their transmitter and receive coverage patterns, transmission power levels, and cochannel interference levels, a wireless connectivity in the form of a dynamic, multi hop graph or as hoc network exists between the nodes. Our approach to communication security in sensor network is based on a basic infrastructure, that says that data items must be protected to a degree consistent with their value. In the particular architecture, for which we are developing our communication security scheme, we differentiate between three types of data sent through the network

- Mobile code
- Locations of sensor nodes
- Application specific data

Following this categorization, we specify the main security threats and appropriate security mechanism:

- Fabricated and malicious mobile code injected into a network can change the behavior of the network in unpredictable ways.
- Acquiring locations of sensor nodes may help an adversary to discover locations of sensor nodes easier than using radio location techniques.
- Protection of application specific data depend on the security requirements of a particular application. In a target tracking application, which was a test case for the given security scheme, we treated the application specific data as the least sensitive type of data.

IV. Security Issues for Mobile Ad Hoc Networks

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.

V. Communication Security Scheme

We define the three types of data in the sensor network, and the possible threats to the network, and the possible threats to the network, in this section we define the elements of the security based on private key cryptography utilizing group keys. Applications and system software access the security API as a part of the middleware defined by the sensor network architecture. Since all three types of data contain more or less confidential information, the content of all message in the network encrypted. We assume that all sensor nodes in the network are allowed to access the content of any message. As we said before, we only deal with communication security. Protection of data within a node is not discussed here. The deployment of security mechanism in a sensor network creates additional overhead. Not only does latency increase due to the execution of the security related procedures, but also the consumed energy directly decrease the lifetime of the network. To minimize the security related costs we propose that the security overhead, and consequently the energy consumption, should correspond to sensitivity of the encrypted information. Following the taxonomy of the types of data in the network, we define three security levels.

- Security I : is reserved for mobile code, the most sensitive information sent through the network

: The messages that contain mobile code are less frequent than the messages that the application instances on different nodes exchange. It allows us to use a strong encryption in spite of the resulting overhead. For information protected at this security level, nodes use to the current master key. The set of master keys, the corresponding pseudorandom number generator, and a seed are credentials that a potential user must have in order to access the network.

- Security II : is dedicated to the location information conveyed in message.

For data that contains locations of sensor nodes, we provide a novel security mechanism that isolates parts of the network, so that breach of security in one part of the network does affect the rest of the network. According to our assumptions about the applications expected to run in sensor networks, locations of sensor nodes are likely to be included in the majority of messages. Thus, the overhead that corresponds to the encryption of the location information significantly influences the overall security overhead in the network.

- Security III : is applied to the application specific information

We encrypted the application specific data using a weaker encryption than the one used for two types of data. The weaker encryption requires lower computational overhead for application specific data. Additionally, the high frequency of messages with application specific data prevents using stronger and resource consuming encryption. Therefore, we apply an encryption algorithm that demands less computational resources with a corresponding decrease in the strength of security

VI. Simulation results

We study the practical impacts of the attacks and examine our analysis through simulation. Two attacks on AODV(Ad Hoc On-demand Distribute Vector and DSDV(Destination Sequence Distance Vector) are considered. We study the practical impacts of the attacks and examine our analysis through simulation. Table 1 lists the simulation parameters that we use.

Table 1. simulation parameters

simulator	2ns
examined protocols	AODV, DSDV
simulated attacks	false distance vector
simulation duration	1000 s
simulation area	1000 * 1000 m
number of mobile hosts	30
transmission range	250 m
movement mode	random waypoint
maximum speed	5 - 20 m/s
traffic type	축(U에)
data payload	512 bytes
packet rate	2 pkt / s
number of malicious host	1
host pause time	10 seconds

The choices of the parameters consider both accuracy and efficiency of the simulation. The host moving speed covers a range from human jogging to vehicle riding in country field. Faster speed is not considered because the frequency of route changes will confuse the performance degradation caused by attacks. The packet rate is chosen to avoid congestion even when there are multiple connections converging at the same host. We choose the following metrics to evaluate the impacts of attacks:

(1) packet delivery ratio
(2) false routing packets sent by the attacker
(3) the number of normal hosts that are cheated by the false routes

Metric(1) is selected to evaluate the percentage of packets that are affected by the attacks. This can be viewed as the strength of an attack. Metric(2) is used to examine the communication overhead of different attacks. Metric(3) examines the propagation of false routes and the potential impacts that are not shown by metric 1.

We consider that the delivery ratio versus the maximum speed of hosts under of attack the conditions. The delivery ratio of attack free AODV keeps high, which shows that the mobility of host is still within the suitable serving range of AODV. DSDV has a slower response to link changes caused by host movement, so the delivery ratio decreases faster

Reference

[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

[4] C. Perkins and E. Royer, "As Hoc on D드몽 Distance Vector Routing, "Proc, Second IEEE Workshop on Mobile Computing Systems and Appliction, IEEE Computer Society Press, Feb, 1999

[5] W. Stallings, Network and Internetwork Security, IEEE Press, 2 edition, 1995