무선 Ad-Hoc 망의 프로토콜 설계 및 보안 모델 해석

김정태
목원대학교

Analyses of Security Model and Design of Protocol for Wireless Ad-Hoc Network

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

Abstract

Ad-Hoc networks are a new generation of networks offering unrestricted mobility without any underlying infrastructure. Primary applications of Ad-Hoc networks are in military, tractical and other security sensitive operations, where the environment is hostile. Hence, security is a critical issue. In this paper, we ahve identified certain misbehaviors caused by mallicious node for reactive routing protocol. We also discuss the intrusion detection and intrusion prevention model to prevent several identified attacks in the networks

Ⅰ. Introduction

There has been explosive growth in the use of wireless communications over the last few years, from satelite trnasmission to home wireless personal area network. The primary advantages of a wireless network is the ability of the wireless node to communicate with the rest of the world while being mobile. T재 basic system models have been developed for the wireless network paradigm. The fixed backbone wireless system model consists of a large number of mobile modes and relatively fewer, but more powerful, fixed nodes. These fixed nodes are hard wired using landlines. The communication between a fixed node and a mobile node within its range occurs via the wireless medium. However, this requires a fixed permanent infrastructure. Another system model, the mobile ad hoc network(MANET) has been peoposed to set up a network when needed. A MANET is considered a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration

Ⅱ. Concepts of Sensor Networks

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.

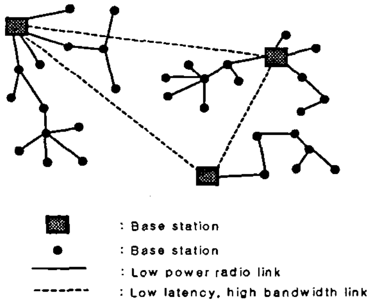
▨ : Base station
● : Base station
—— : Low power radio link
------- : Low latency, high bandwidth link

Figure 1. A representative sensor network architecture

III. A Mobile Routing Infrastructure

Each node in a moblie 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, dependending on the nodes positions, their trnasmitter and receive converage patterns, transmission power levels, and cochannel interference levels, a wireless connectivity in the form of a dynamic, multihop 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 paticular architectre, for which we are developing our communication security scheme, we differentiate between three types of data sent through hte network

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

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

- Fabracated 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 noodes easier than using radio location techniques.
- Protection of application specific data depend on the security requirements of a paticular applicaiton. In a target tracking application, which was a test case for the given security scheme, we treated the application sepecific data as the least sensitive type of data.

IV. Security Issues for Mibile 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;

1) *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.

2) 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.

3) 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.

4) 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.

5) Forwarding

Nodes can decide to forward messages to partners in collusion for analysis, disclosure, or military benefits.

V. Construction Issues in Address Architectures

While still an open issue within the working group, it is recognized that a sufficient addressing architecture should support the following capabilities.

- *interoperability via adherence to the IP addressing architecture*
- simultaneous use of multiple wireless technologies
- the presence of multiple hosts per router

These capabilities can be realized by an architecture as shown belows.

- identifies end hosts with IP addresses
- identifies a Manet node with a node ID
- allows advertisement of multiple hosts and subnets per Manet node.

VI. 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

참고문헌

[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 D 드뭉 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