무선 이동 Ad hoc 네트워크에서의 보안성 문제 분석

김정태
목원대학교

Analyses of Security Issues in Wireless Mobile Ad Hoc Network

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

요 약

A s wireless communications and mobile multimedia services are booming nowadays, systematic research of the overall aspects of mobile security is crucial. This paper presents a frame model for guising the systematic investigation of mobile security. Based on the introduction of some background viewpoints of security targets from n novel perspective, the framework is described as a hierarchical model in which mobile security research is partitioned into three different layers.

I. Introduction

Mobile code has a long and varied history, beginning with computing pioneer John von Neumann's seminal concept of one automaton controlling another. In the 1960s, the mobile code idea was evident in remote job-entry terminals that transferred programs to mainframe computers. Ten years later, Ukrainian researcher Peter Sapaty introduced the Wave system, which offered full mobile code functionality.1 In the 1980s, Scandinavian packet-radio enthusiasts developed a Forth-based approach to remotely transferring and executing programs through a wireless infrastructure. In the 1990s, Sun Microsystems introduced Java, marking the first widely used mobile code implementation. Along the way, mobile code has been viewed using different perspectives and paradigms. Unlike mobile computing, in which hardware moves,2 mobile code changes the machines where the program executes. Ubiquitous computing or Active Information Spaces promote the proliferation of embedded devices, smart gadgets, sensors and actuators. We envision an Active Information Space to contain hundreds, or even thousands, of devices and sensors that will be everywhere, performing regular tasks, providing new functionality, bridging the virtual and physical worlds, and allowing people to communicate more effectively and interact seamlessly with available computing resources and the surrounding physical environment. This vision of Active Information Spaces is not far fetched; the Gaia project [1] [2] [3] at the Department of Computer Science, University of Illinois at Urbana-Champaign, attempts to develop a component based, middleware system that provides support for building, registering and managing applications that run in the context of Active Information Spaces. However, the reallife deployment of Active Information Spaces is hindered by poor and inadequate security measures, particularly, authentication and access control techniques. Active Information Spaces promote the automation of some services (e.g. automatic adjustments of lighting and air conditioning), and the anytime, anywhere access to resources, in an attempt to enhance users' productivity and services' availability.

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.

III. Design Strategy

Security design in such infrastructure wireless mobile networks is challenging for several reasons.

1) Security beach: wireless transmissions are prone to security attacks, and it is very likely that adversaries will eventually break into a limited number of entities over a large time window.

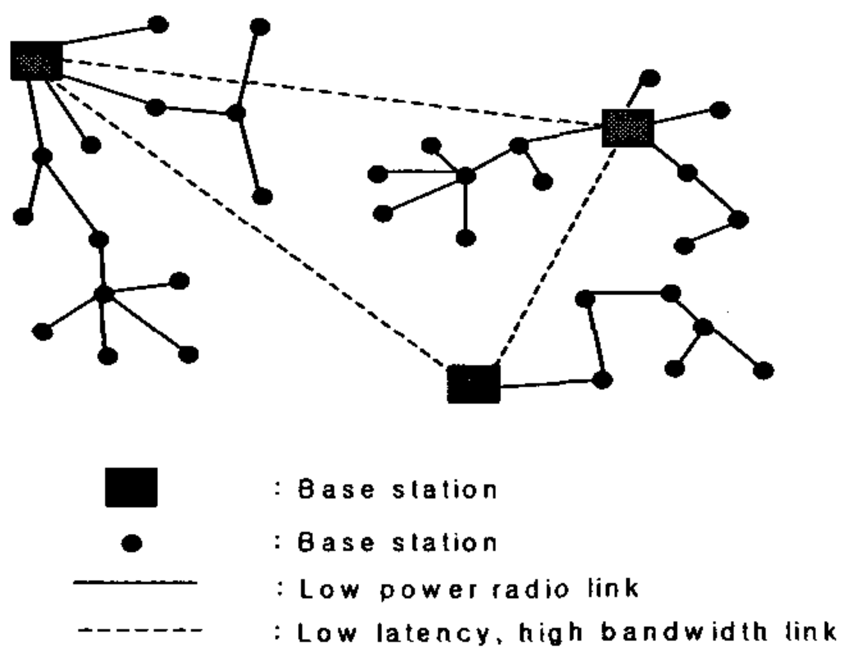
■ : Base station
● : Base station
—— : Low power radio link
------- : Low latency, high bandwidth link

Fig 1. A representative sensor network architecture

2) Mobile and security ubiquity: Mobile users incur dynamic tpological changes. A mobile user may be able to perform effective and timely communication with its local neighbors but not with remote entities. For example, routing protocols may fail to establish robust communication over multi-hop paths, as it is the case with DSR, which is limited to 10 hop scenarios.

3) Network dynamics: Channel errors, and node failures all incur dynamics into the network. Besides, an entity may join and leave the network over time.

4) Network scale: The number of networking devices can be large, thus a scalable solutions is critical.

IV. Special Security Issues for Mobile Ad Hoc Networks

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

1) Cooperation and fairness

There is a trade-off between good citizenship, i.e. 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 service. 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; incorrect forwarding; and bogus routing advertisement.

2) Confidentiality of location:

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

3) No traffic diversion:

Routes 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:

V. Security Vulnerability in Mobile Ad hoc Networks

A malicious node can disrupt the routing mechanism employed by several routing protocols in the following ways.
Attack the route discovery process by:

- Changing the contents of a discovered route
- Modifying a route reply message, causing the packet to be dropped as an invalid packet
- Invalidating the route cache in other nodes by advertising incorrect paths
- Refusing to participate in the route discovery process. Attack the routing mechanism by:
- Modifying the contents of a data packet or the route via which that data packet is supposed to travel
- Behaving normally during the route discovery process but drop data packets causing a loss in throughput Generate false route error messages whenever a packet is sent from a source to a destination. Launch DoS attacks by:
- Sending a large number of route requests. Due to the mobility aspect of MANETs, other nodes cannot make out whether the large number of route requests are a consequence of a DoS attack or due to a large number of broken links because of high mobility.
- Spoofing its IP and sending route requests with a fake ID to the same destination, causing a DoS at that destination.

VI. Intrusion Detection in MANETS

Quite a bit of research work has already been done in intrusion detection for traditional wired networks. However, applying the research of wired networks to wireless networks is not an easy plug-and-play task because of key architectural differences, principal among them being the lack of fixed infrastructure. The absence of physical infrastructure facilitates the attacker's task since it is easier to eavesdrop on network traffic in a wireless environment. Wireless ad hoc networks, due to their vulnerabilities, provide a tougher challenge for designing an IDS. Without centralized audit points such as routers and gateways, an IDS for ad hoc networks is limited to using only the current traffic coming in and out of the node as audit data. Another key requirement is that the algorithms the IDS uses must be distributed in nature, and should take into account the fact that a node can only see a portion of the network traffic. Moreover, since ad hoc networks are dynamic and nodes can move about freely, there is a possibility that one or more nodes could be captured and compromised, especially if the network is in a hostile environment. If the algorithms of the IDS are cooperative, it becomes important to be skeptical of which nodes one can trust. Therefore, intrusion detection systems on ad hoc networks have to be wary of attacks made from nodes in the network itself, not just attacks from outside the network. Also, mobile networks cannot communicate as frequently as their wired counterparts to detect intrusions in order to conserve bandwidth resources. Bandwidth and other issues such as battery life compound the problem even further. The availability of partial audit data makes it harder to distinguish an attack from regular network use.

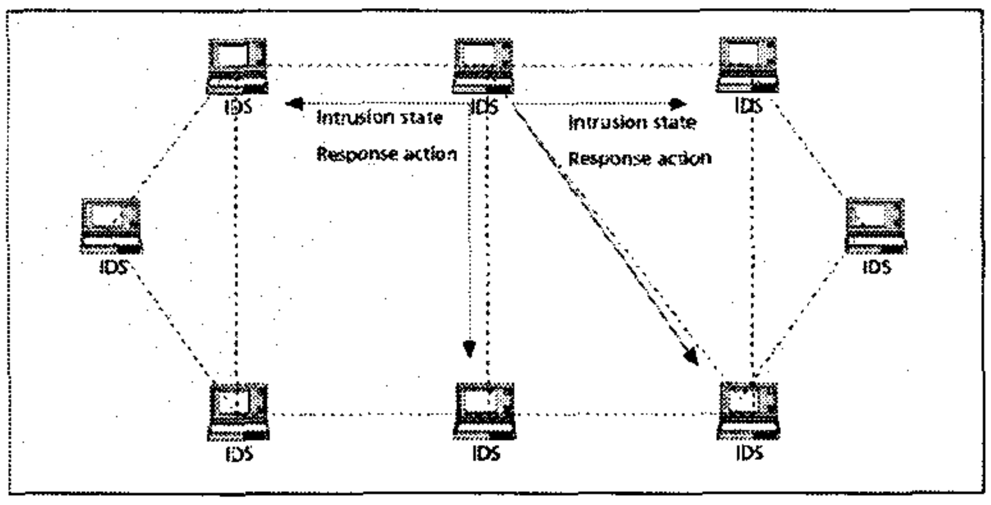

Fig 2. IDS architecture for a wireless ad hoc network.

VII. Conclusion

In this paper, we have discussed the security challenges imposed on ad hoc networks. A Security requirements for Ad Hoc Wireless System mechanism have been proposed. We believe that the integration and adaptive nature of mobile would bring more robust defense to ad hoc networks.

References

[1] G. Borriello, “Key Challenges in Communication for Ubiquitous Computing,” IEEE Comm. Mag., May 2002, pp. 16-18.

[2] F. Stajano and R. Anderson, “The Resurrecting Duckling: security issues for ubiquitous computing,”Computer , Vol.: 35 Iss. 4 , April 2002, pp. 22 -26.

[3] W. Feng, "Securing wireless communication in heterogeneous environments", MILCOM 2002 - IEEE Military Communications Conference, no. 1, October 2002 pp. 1101-1106

[4] J. Li, S. B. Weinstein, J. Zhang and N. Tu, “Public access mobility LAN: Extending the wireless internet into the LAN environment”, IEEE Wireless Communications, vol. 9, no. 3, June 2002, pp. 22 - 30