이종 시스템 환경하에서의 무선 네트워크의 보안 대책

김정태

목원대학교

Analyses of Wireless Network Security in Heterogeneous Environments

Jung-Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

With the convergence of mobile devices and the Internet ubiquitous computing promises to revolutionalize the way that we access services and run application. However, ubiquitous computing environments, in particular, mobile and wireless environments interfaced with the Internet, currently possess security vulnerabilities that are ripe for attack from cyber-threats. Thus, this paper discusses the limitation of current security mechanisms in ubiquitous computing environments

I . Introduction

Rapid advances in mobile devices and wireless networking have converged to enable ubiquitous computing where mobile dvices can access services, run programs, utilize resources, and harvest computing power anytime and anywhere. This new generation of ubiquitous and mobile computing enables the delivery of services that are no longer bound by time or location barriers. For the general public, this may provide the ubiquitous delivery of integrated services and multimedia enabled applications to home. For the military, it can enable the reconnaissance of enemy movement via wireless sensor network.

II. Infrastructure

A. Lack of Reconfigurability

Imposing a fixed standard or fixed protocol for securing wireless communication leads to system that are inflexible. Furthermore, such systems can become unusable whenever a security flaw is discovered in the protocol or in any one of the employed cryptograhic algorithm. Ubiquitous computing environments need security services that can be dynamically reconfigured, thus allowing them to adapt to different scenarios, security requirements and computing resources.

B. Complexity of Security Level

Security gaps appear when a secure session terminates prematurely. Such terminations occur in ubiquitous computing environments due to the multimode nature of the communication link between the mobile device and its final destination, resulting in security gaps that can expose sensitive data.

Nowdays, 3G's architecture generally uses IPSec only between different networks and is not truly end to end. In some cases the

deployment of IPSec will only occur between the visited and home networks.

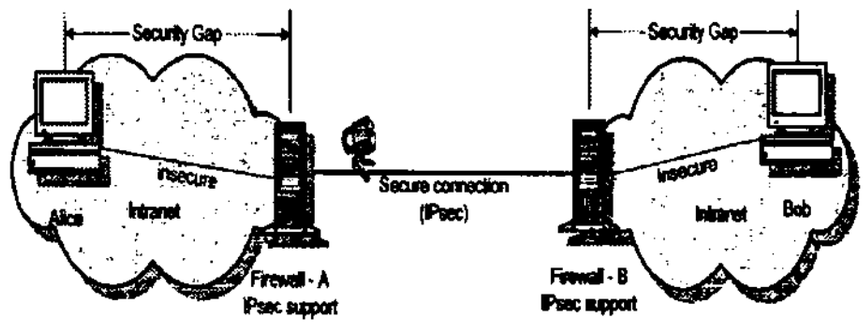

Fig 1. Example of security gap level

Security level are introduced whenever data packets have to pass through different network realms such as heterogeneous environments. Special devices at the realm boundaries exist to handle the diversity between realms. These devices transparently fix packet flows between endpoint, handle data transition between realms, and provide mobility support, address translation, packet filtering, and data compression.

C. Analyses of Communication Protocol

Many existing security protocols depend on a particular communication protocol. This dependancy limits their portability to other networking infrastructure. For example, IPSec is inherently dependent on IP. However, many wireless environments do not use IP for communication such as WAP and wireless sensor networks.

Mobile ad hoc networks(MANETs) are vulnerable to the same threats as any wireless networks. However, due to their nature there are also some additional threats and vulnerabilities. In general, the research has noted that traditional security solutions, such as public key infrastructures or authentication mechanisms, also have potential for MANETs but in many cases they are not sufficient by themselves. Overviews of the research efforts can be found. The following list points out the main properties of the ad hoc paradigm:

o Lack of central administration; no central administration, control or prior contact is assumed;

o Routing mechanisms are more vulnerable than in conventional networks because each node can act as a relay;

o Co-operation: if a node does not respect the cooperation rules - i.e. it is selfish - the performance
of the network can be severely affected;

o Variation in memory and computation resources: many of the nodes are expected to be low-priced consumer electronics with cheap and slow computation capability and limited storage size; and

o Energy constrained operation: many of the nodes are expected to operate on battery power. Sleep or standby modes are used to conserve energy, during which they may not be reachable. Sleep deprivation torture (exhausting battery power) attack is used by attackers.

III. Summary of requirements

To summarize the requirements, the following points, from our point of view, should be carefully treated in future research.

☐ provide seamless mobility over heterogeneous networks with sufficient security but no apparent performance compromise

☐ mobility vs. location privacy

☐ anonymity vs. accountability

☐ ensure that service provided to users through 3rd parties are trustful, because user will most possibly complain to mobile network operator when they have a problem

☐ special terminal features and reconfigurability vs. security: user may buy mobile devices directly from vendors

instead of from operators, the issue here is security for heterogeneous devices

□ last but not least we should not forget that, human being and software bugs can be the weakest link in security Each node in a mobile as hoc network logically consists of a router with possibly IP addressable hosts and multiple wireless

- Locations of sensor nodes
- Application specific data

Security network functional model and threats is presented. To study security in roaming service provision, it is required to extract the network functional entity and establish a network functional model to clarify security functional allocation. The treats in each functional entity to be studied are as follows.

a. treats on interworking between user and terminal:
b. treats on interworking between terminal and visited network
c. Threats on interworking within network
d. Threats on interworking between network
e. Threats on interworking between operator and database

IV. Node Level Security Monitoring

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.

The basis of security monitoring is security metrics. A compositional approach can be used to define security metrics for mobile ad hoc networks with the following, possibly iterative, steps:

1. Define security objectives: the security objectives can be defined based on the knowledge of the security environment, assumptions and threats. Among other things, they should determine the required security level;
2. Select component metrics based on the security objectives;
3. Find cross-relationships (dependencies) between the component metrics and possibly re-define component metrics as independently as possible;
4. Compose integrated security level information: the final composition mainly depends on the method of measurement. The composition can be used for both quantitative and qualitative security metrics.

V. Security Threats

Wireless networks, in general, are more vulnerable to security attacks than wired networks, due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. To demonstrate, on an example, some of the security threats and our corresponding protection mechanisms. The nodes that detect a target in an area exchange messages containing a timestamp,

the location of the sending node and other application-specific information. When one of the nodes acquires a certain number of messages such that the location of the target can be approximately determined, the node sends the location of the target to the user. Not only the application messages are exchanged through the network, but also mobile code is sent from node to node. Because the security of mobile code greatly affects the security of the network, we consider protection of the messages containing mobile code as an important part of our communication security scheme. We list the possible threats to a network if communication security is compromised:

1. Insertion of malicious code is the most dangerous attack that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary. A seized sensor network can either send false observations about the environment to a legitimate user or send observations about the monitored area to a malicious user.
2. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. The significance of hiding the location information from an attacker lies in the fact that the sensor nodes have small dimensions and their location cannot be trivially traced. Thus, it is important to hide the locations of the nodes. In the case of static nodes, the location information does not age and must be protected through the lifetime of the network.
3. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. Confidentiality of those fields in our example application is less important then confidentiality of location information, because the application specific data does not contain sensitive information, and the lifetime of such data is significantly shorter.
4. An adversary can inject false messages that give incorrect information about the environment to the user. Such messages also consume the scarce energy resources of the nodes.

VI. Conclusion

In this paper, we propose a communication security scheme for sensor networks. The straightforward approach to the secure communication in sensor networks could be the application of a single security mechanism for all data in the network. However, if the mechanism is chosen according to the most sensitive data in the network, security related resource consumption might be unacceptable. Thus, in this paper, we discusses the limitation of current security mechanisms in ubiquitous computing environments

References

[1] Tilmann H, "On/off phase shift keying for chaos encrypted communication using external cavity semiconductor lasers". IEEE J. of QE, v.38, n.9, sep. 2002, pp.1162-1170

[2] Shuo T, "Effects of message encoding and decoding on synchronized chaotic optical communication", IEEE J. QE, v.39,n.11, Nov, 1003, pp1468-1474

[3] V. Raghunathan, C. Schurgers, S. Park, M. B. Srivastava, “Energy-aware wireless microsensor networks”, IEEE Signal Processing Magazine, vol.19, (no.2), IEEE, March 2002. pp. 40-50.