무선 센서 네트워망에서의 보안 메카니즘 분석

김정태
목원대학교

Analyses of Security Mechanism for Wireless Sensor Network

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

요 약

Sensor networks will play an important role in the next generation pervasive computing. But its characteristic of wireless communication brings a great challenge to the security measures used in the communication protocols. These measures are different from conventional security methods. In this paper, we proposed a security architecture for self-organizing mobile wireless sensor networks. It can prevent most of attacks based on intrusion detection

I . Introduction

Many sensor networks have mission-critical tasks, it is clear that security needs to be taken into account. The information leakage may be occurred when sensor nodes used to monitor the surroundings. More over, the wireless communication employed by sensor networks facilitates eavesdropping and packet injection by an adversary. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. The attractive features of the wireless sensor networks attracted many researchers to work on various issues related to these types of networks. However, while the routing strategies and wireless sensor network modeling are getting much preference, the security issues are yet to receive extensive focus. Mobile ad hoc networks and wireless sensor networks have promised a wide variety of applications. However, they are often deployed in potentially adverse or even hostile environments. Therefore, they cannot be readily deployed without first addressing security challenges. Intrusion detection systems provide a necessary layer of in-depth protection for wired networks. The general accepted definition for a wireless sensor network consists of the formation of a communication network among many low-cost, low-power wireless sensing devices throughout a physical area . It is also assumed that the sensors are scattered randomly in a planar area and there are sufficiently enough sensors to create many redundant communication paths once they have been placed. It is also assumed that they are immobile. This definition of wireless sensor networks does not match with what we envision in order to be deployed in a disaster evaluation and recovery sensory network.

II. Attacks on Each Layers

The security architecture of wireless sensor networks is difference from other kinds of networks due to the resource limitations of sensor nodes. That makes us particularly hard to design an idle security architecture for the whole layers. According to the OSI model, we divided the security architecture into five layers, as depicted in Fig.1. Each layer has its own attack types and countermeasures are taken according to the specific layers. Most sensor nodes are in hibernation state under normal situation in order to save energy. When emergent events happen, sensors need to be activated immediately. At the same time, the detection module must start to monitor the security status in the network.

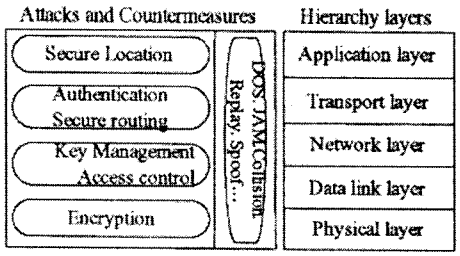

Fig 1. The security architecture of WSN

1) Data Link Layer Security

Security in the Data Link Layer provides hop-to-hop protection (encryption and authentication), with no user or application authentication.

Security provided by Bluetooth, Zigbee or the public mobile telephony network, in each case, is an example

of Data Link Layer protection.

2) Network Layer Security

Security in the Network Layer provides node-to-node protection (encryption and authentication), with no user or application authentication. The node-to-node protection in the network layer can be hop-to-hop protection or end-to-end protection. For the Network Layer protection, IPsec is an example, which can be used between systems using static IP addresses.

3) Transport Layer Security

Security in the Transport Layer provides an end-to end protection. It provides application-to-application protection, and it can also include user authentication. SSL/TLS or HTTPS are examples of Transport Layer security.

4) Application Layer Security

Security in the Application Layer provides application to application and application-user to application-user protection, including user (sender and receiver) authentication. Application Layer security is provided through the encryption (symmetric or asymmetric) or/and signature of the data sent through the communications stack.

SMIME or user-invoked cryptographic functions (e.g. OpenSSL) are examples of tools that can be used to encrypt and sign data for the Application Layer security.

III. Security Threats and Issues in Wireless Sensor Networks

Wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In most of the cases various security issues and threats related to those we consider for wireless ad hoc

networks are also applicable for wireless sensor networks.

1) Attacks in Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here we point out the major attacks in wireless sensor networks.

2) Attacks on Information in transit

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks

3) Sybil Attack

The sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes

IV. Security Requirements for WSNs

The security services of ad hoc networks are not altogether different from those of other network. The goal of these services is to protect information and resources from attacks and misbehavior. In dealing with network security, we will explain the following requirements that an effective security architecture must ensure:

1) Availability:

Ensures that the desired network services are available whenever they are expected, in spite of the presence of attacks. Systems that ensure availability in MANETs seek to combat denial of service and energy starvation attacks, as well as node misbehavior such as node selfishness in packet forwarding. All these threats will be presented later.

2) Authentication:

Ensures that communication from one node to another is genuine. In other words, it ensures that a malicious node cannot masquerade as a trusted network node.

3) Data confidentiality:

Ensures that a given message cannot be understood by anyone other than its (their) desired recipient(s). Data confidentiality is typically enabled by applying symmetric or asymmetric data encryption.

4) Integrity: Denotes the authenticity of data sent from one node to another. That is, it ensures that a message sent from node A to node B was not modified by any malicious node C during its transmission. If a robust confidentiality mechanism is employed, ensuring data integrity may be as simple as adding one-way hashes [1] before encrypting messages.

5) Non-repudiation: In computer networks, non-repudiation is the ability to ensure that a node cannot deny the sending of a message that it originated. Digital signatures may be used to ensure this.

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. Conclusion

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. Many of today's proposed security schemes are based on specific network models. We reviewed the security threats, security mechanisms for wireless sensor networks. We also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks.

References

[1] H.Chan and A.Perrig, "Security and Privacy in Sensor Networks," IEEE Computer, vo.36, no.10, pp103-105, October 2003.

[2] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[3] Zhou, L. and Haas, Z. J., "Securing ad hoc networks", IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24 - 30.

[4] Nikola Milanovic, Miroslaw Malek, Anthony Davidson and Veljko Milutinovic, "Routing and Security in Mobile Ad Hoc Networks," IEEE Computer, Vol. 37, No. 2, pp. 61-65, February 2004.

[5] IEEE mobile standards web page: http://standards.ieee.org/mobile/overview.html#802.15