Design of Integrated Security Framework for Open Wireless Networking Architecture

김정태

목원대학교

공개 무선 통신망 구조를 위한 복합 보안 프레임워크 설계

Jung-Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

An integrated security mechanism is one of the key challenges in the open wireless network architecture because of the diversity of the wireless network in open wireless network and the unique security mechanism used in each one of these networks. Optimized security protocols and mechanisms are employed for the high performance and security. Finally, a challenge in the near future will converge the integration of Open Ubiquitous Sensor Network (OUSN) with security protocols for applying the their applications. We analysed unique network-centric features and security mechanism of various heterogeneous wireless networks.

Ⅰ. Introduction

To integrate several open wireless network into single networks, a lot of consideration should be taken into account to solve challenges that must be addresses. These matters include support for mobility management, quality of service provision, and security interoperability. An integrated security mechanism is one of the key challenges in open wireless network architecture because of the diversity of the networks in open wireless network architecture and the unique security mechanism used in each of the networks.

II. Related Work

In the 21st century, advanced technologies have developed with fusion technology related to IT and another fields of technology. The inherent and open quite fundamental differences among the various OUSN related wireless networks, integration of the security schemes of those networks is not easy job. We analyse some of those differences.
- Architecture characteristics
- Security requirements
- Selected security mechanism and standards

III. Basic Security Concepts

Security of wireless networks can be more easily compromised and may be vulnerable to a more diverse range of

threats than wired networks. The generic security requirements are as follows.
- Confidentiality
- Authentication
- Integrity
- Availability
- Non-repudiation

Security technology can be implemented with cryptographic mechanism. Cryptographic is composed of two processes, encryption and decryption. The popular techniques are private key cryptosystem and public key cryptosystem.

IV. Security features and mechanisms of OUSN

We analysed to implement an architecture based on OUSN related wireless networks with specialized features.
- Security of cellular networks
- WLAN security
- Security of AD networks
- Key distribution
- Secure routing protocols
- Security of sensor networks
- RFID security
- Non-cryptographic schemes
- Lightweight cryptographic schemes
- Conventional cryptographic schemes

A. Fundamental security approaches
- Multiple security mechanisms for source to destination security
- Evolution from the notion of security mechanisms to the notion of security management
- Upper layer security approach
- Multiple independent security processes

B. Analyses of integrated security procedure
- User to device
- Sensor device to sink or RFID tag to reader
- Sensor networks to AD Hoc network
- - Ad Hoc networks to WLAN

- WLAN to cellular network

V. Conclusion

In this paper, we analysed several cryptographic algorithms using measurements on real sensor hardware. The selected algorithms build the basis for nearly any security solution used in communication networks including wireless ad hoc and sensor networks.

References

[1] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal of selected areas in communications, V.24, N.2, pp.381-394, February, 2006
[2] D. Djenouri and L. Khelladi. A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks. IEEE Communication Surveys and Tutorials, V.7, N.2., pp.2-28, December 2005.
[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. SPINS: Security Protocols for Sensor Networks. Wireless Networks, V.8., N.5., pp.521 - 534, September 2002.
[4] Mykletun, E., Girao, J., and Westhoff, D., "Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks," Proceedings of IEEE International Conference on Communications, 2006, pp. 2288-2295.

Acknowledgement