Analyses of Dynamic Crypto Mechanism in Sensor Network Security

김정태
목원대학교

센서 네트워크 보안을 위한 정적인 보안 메카니즘에 대한 분석

Jung-Tae Kim
Mokwon University
E-mail : jtkim5068@gmail.com

요 약

Security has become a major concern for many real world applications for wireless sensor networks. Usually, all these approaches are based on well known cryptographic algorithms. At the same time, performance analyses have shown that the applicability of sensor networks strongly depends on effective routing sessions or energy aware wireless communication. Based on our experiments, we provide some analyses and considerations on practical feasibility of such cryptographic algorithms in sensor networks.

Ⅰ. Introduction

Recent progress in wireless communications and micro electro mechanical systems technology has made it feasible to build miniature wireless sensor nodes that integrate sensing, data processing, and communicating capabilities. These miniature wireless sensor nodes can be extremely small, as tiny as a cubic centimeter. Compared with conventional computers, the low-cost, battery-powered, sensor nodes have a limited energy supply, stringent processing and communications capabilities, and memory is scarce. The design and implementation of relevant services for WSNs must keep these limitations in mind.

II. Security Solutions and Architectures

The primary requirements on a successful security architecture for sensor network are availability, authentication, data confidentiality, integrity, and non-repudiation. Most of these objectives can be addressed using cryptographic hash functions and appropriate encryption schemes. In ad hoc and sensor networks, many proposals were published concerning the use of security measures for particular applications. Security protocols such as define complex architectures to be used in a sensor network environment. Most of such proposals defer the problem of key management, one of the most sophisticated problems to be solved elsewhere. Fortunately, several approaches seem to be adequate in this domain. One example is the efficient public-key encryption in sensor networks. A survey on key management solutions can be found in.[2]
In summary, it can be said that many promising proposals can be found in the literature that address the security objectives in sensor networks. Nevertheless, most of these papers only outline the principles or use simulation environments for verification. We tried to verify the applicability of such solutions on real

sensor node hardware by analyzing the performance of several cryptographic algorithms. In particular, we selected the following three cryptographic algorithms:

MD5 (Message Digest)

SHA-1 (Secure Hash Algorithm)

AES (Advanced Encryption Standard)

The first two algorithms, MD5 and SHA-1, represent cryptographic hash functions that are heavily used for typical message integrity checks and authentication. AES is a symmetric encryption algorithm that promises fast operation compared to asymmetric solutions.[1]

III. Research Issues in Wireless and Sensor Networks Security

The objective of this section is to review the main research domains in wireless and sensor networks security that have been addressed in the past years.[2] Before introducing individual contributions, we first summarize the research domains addressed by WSNS papers in the last three years. In particular, the following seven domains have been addressed:

Key management Key management is still one of the most challenging issues in ad hoc networks. The question is how do multiple nodes establish shared keys and how they can revoke keys if necessary.

Performance and scalability Focusing on low resource sensor networks, the performance of secure communication protocols and cryptographic algorithms needs to be considered for developing practical secure applications.

Access control and authentication Access control and authentication in wireless networks is difficult as usually no complex security architectures such as IPSec or Kerberos are available.

Security protocols Agreement protocols and integrated reliability and security measures are needed indistributed low resource networks.

Routing and clustering Ad hoc routing in wireless networks requires countermeasures against two different threats. First, selfish nodes exhaust resources from the entire network without delivering any service and, secondly, routing protocols can be attacked to eaves-drop information packets.

Secure localization Localization is a major research issue in ad hoc and sensor networks. If no security measures are integrated, this essential component can not be trusted.

Intrusion detection Attacks such as address spoofing, denial of service, and general misbehavior need to be detected early in order not to spend too much resources for transporting attack packets.

IV. Conclusion

We analyses to use our measurement results as a basis for validating security scenarios for wireless sensor networks. Real measurements must build the basis for analyzing proposed security protocols in order to estimate their behavior. Additionally, our measurement results can be used to calibrate simulation setups in order to find out boundaries for real-time operation and communication.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A Survey on Sensor Networks. IEEE Communications Magazine, 40(8):102 116, August 2002.

[2] D. Djenouri and L. Khelladi. A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks. IEEE Communication Surveys and Tutorials, 7(4):2 28, December 2005.