RFID와 무선 센서네트워크를 융합한 프로토콜에서의 보안 문제

김정태

목원대학교

Security Issues in Combined Protocol Between RFID Application and Wireless Sensor Network

Jung Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

본 논문에서는 무선 센서네트워크망을 이용한 헬스케어 시스템에서의 사용자 인증을 위한 프레임에서의 보안 문제를 해석하였다. 이러한 메디컬 센서 데이타는 환자의 몸으로 부터 신호를 받아 의사 등과 스태프에게 정보를 전달한다. 개개인의 정보가 취약성을 가지고 있으며, 비 인가된 제 3자에게 노출되고 있다. 따라서, 본 논문에서는 두 가지의 요소를 가진 사용자 인증 프로토콜을 설계할 때 문제시 되는 방법을 분석하였다. 또한 이러한 프로토콜에서 발생 가능한 위협 요소를 정의하였다.

ABSTRACT

This paper presents a user authentication scheme for healthcare application using wireless sensor networks, where wireless sensors are used for patients monitoring. These medical sensors' sense the patient body data and transmit it to the professionals. Since, the data of an individual are highly vulnerable; it must ensures that patients medical vital signs are secure, and are not exposed to an unauthorized person. In this regards, we propose a user authentication scheme for healthcare application using medical sensor networks. The proposed scheme includes: a novel two-factor user authentication, where the healthcare professionals are authenticated before access the patient's body data; a secure session key is establish between the patient sensor node and the professional at the end of user authentication. Furthermore, the analysis shows that the proposed scheme is safeguard to various practical attacks and achieves efficiency at low computation cost.

키워드

RFID, Security Protocol, WSN, USN

Ⅰ. Introduction

Recent advances in wireless networks and embedded systems have created a new class of pervasive systems such as Wireless Sensor Networks (WSNs) and Radio Frequency IDentification (RFID) systems. WSNs and RFID have made a variety of new and exciting applications, particularly for pervasive computing. For example, WSNs have been used in areas such as health monitoring. The wireless broadcast nature may result in privacy breaches of sensitive information during data transmission. Therefore, security and privacy issues of WSNs have attracted a lot of research efforts. Bo Sun, etcs, briefly introduced WSNs

and RFID systems. We then present their security concerns and related solutions. Finally, he propose a Linear Congruential Generator (LCG) based lightweight block cipher that can meet security co-existence requirements of WSNs and RFID systems for pervasive computing. [1]. Hung-Yu Chien and Chi-Sunbg Laih proposesd a new RFID authentication protocol based on Error Correction Codes (ECC). The proposed scheme has excellent performance in terms of security, efficiency, server's maintenance, robustness, and cost. The tag only performs simple operations, such as random number generation and simple bitwise computations. The lightweight feature makes it attractive to those low-cost RFIDs that support only simple operations [2].

Ⅱ. Security Issues on Wireless Sensor Network and RFID Application

One WSN may be composed of hundreds or thousands of miniature sensor nodes, or motes, which are fitted with an on-board processor. The wireless broadcast nature may result in privacy breaches of sensitive information during data transmission. Therefore, security and privacy issues of WSNs have attracted. The representative of attacks are as follows.

- Physical attacks
- Attacks at physical layer
- Attacks at link layer
- Attacks at network layer
- Attacks targeting at WSN services and applications

Ⅲ. Attacks on RFID System

These countermeasures aim at protecting the integrity, authenticity, and confidentiality of WSNs. An RFID system usually consists of RFID tags and RFID readers. A tag is attached to a physical object and contains a digital number associated with that object. Tags usually have very low cost, limited storage, and extremely limited computing capability. We briefly consider a few security violations that can arise in the presented context and evaluate the proposed protocol [3].

- Denial of Service (DoS)/desynchronization attack:
- Forward Security:
- Replay attack:
- Impersonation attack:
- Tag tracking attack:
- Eavesdropping:

In 2008, a scalable radio frequency identification (RFID) authentication protocol was proposed by Yanfei Liu to provide security and privacy for RFID tags. Imran Erguler and Emin Anarim examine the security of the YL scheme that has received no attacks yet and show that YL mutual authentication protocol is vulnerable to the tag tracking, tag impersonation, and desynchronization attacks [4].

Ⅳ. Conclusion

In this paper, we first briefly presented WSNs and RFID systems and described their privacy and security concerns and related solutions. We finally surveyed a Linear Congruential Generator based lightweight block cipher that can meet security co-existence requirements of WSNs and RFID systems.

References

[1] Bo Sun, Yang Xiao, Chung Chih Li, Hsiao-Hwa Chen and T.AndrewYang, "Security co-existence of wireless sensor networks and RFID for pervasive computing," Computer Communicatioms, p.4294-4303
2008. pp.4294-4303

[2] Hung-Yu Chien and Chi-Sung Laih, "ECC-based lightweight authentication protocol with untraceability for low-cost RFID," Journal of Parallel Distribution Computer,V.69, 2009, pp.848-853

[3] Wei Zhou, Eun Jung Yoon and Selwyn Piramuthu, "Simultaneous multi-level RFID tag ownership & transfer in health care environments," Decision Support System V.54, 2012, pp.98-108

[4] Imran Erguler and Emin Anarim, "Practical attacks and improvements to an efficient radio frequency identification authentication protocol," Concurrency and Computation: Practice and Experience, 2011, pp.100-18

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number: 2013-052980)