© 2020 IJSRST | Volume 7 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : 10.32628/IJSRST

Study of Security Measures and RFID Network

Smita Kumari
M. Phil. Students, Department of Physics, B. R. A. Bihar University, Muzaffarpur-842001, Bihar, India

ABSTRACT

In this paper, we studied about security measures and RFID network. RFID facilitates detection and identification of objects that are not easily detectable or distinguishable by using current sensor technologies. Radio frequency identification (RFID) uses electromagnetic field of radio frequency for automatic identification of objects with a unique ID number which is stored in the attached tag [1]. Both RFID and barcode systems have the same goal; identifying objects without human intervention.

Keywords: RFID, WSN, Radio Waves, Sensor.

I. INTRODUCTION

RFID systems have many continuing and emerging applications like access controls, tool management, supply chains, airline baggage management, livestock or inventory tracking and so on. It can also be used to distinguish between counterfeits and authentic products. The important security and operational problems such as cloning problem, tracing problem and scalability can be solved by RFID system with cheaper RFID tags for commercial application. Security can be CMOS technologies progressively efficient and the production costs decrease, which allows stronger security solutions on tags. More expensive tags with constraints power source, less memory, gate can be used for certain commercial application such as access controls systems and costly goods for security [1] [2].

This section describes a security model. The system consists of three components: a trusted server *S*, reader *R*, and tag *T*.

- Typically Tags have no its own power. It operates on electromagnetic field. These are wireless Trans ponders.
- The fields are generated by the transceiver that is the Reader. There exits two kind of broadcast challenges by responding the tags. These are unicast and multi-cast. Under the range of reader, these are addressed to all tags. But unicast challenges are addressed to particular tags.
- Server: The system has a trusted Server communicates with the reader and also reader communicated with the server. We consider that all honest tags *T* follow the protocol's requirements and system specifications. The parameters fixed are applied to the honest readers *R* and the trusted server *S*. Both Tag *T* and reader *R* interact by sending and receiving of data as an authentication transcript. We assume the communication take place through secure channel. Since two parties involves in this communication, we can consider as two-party protocols.

II. SECURITY ANALYSIS

Here we will analyze how the basic protocol meets the key RFID security requirements. The first requirement is to prevent unauthorized access to the RFID tag information. We first consider an unauthorized reader querying the tag. The adversary will issue its own random number nr, and receive nt, h(s,nr,nt) XOR id from the tag. Since the backend server will not respond to the adversary, the adversary now has to determine id without any help from the backend server. The adversary succeeds if he is able to determine id from nt, h(s,nr,nt) XOR id. In order to get back id, we need to XOR with h(s,nr,nt) using the correct s value, but the adversary only knows nr and nt, and not s. Thus, the adversary is unable to obtain id. Since the protocol uses a conventional hash function such as SHA, the adversary cannot obtain s from h(s,nr,nt). The adversary can attempt to guess the value of s, but this can be defended against by using large enough values of s. Another method of unauthorized access is for the adversary to be eavesdropping when a legitimate reader is querying a tag. Since the wireless channel between the reader and tag is assumed to be insecure, the adversary is able to learn nr, nt, and h(s,nr,nt) XOR id. These pieces of information are similar to that obtained when the adversary queries the tag directly, which yields no useful information
to the adversary.

The second requirement is to prevent illicit tracking. In this attack, the adversary needs to determine whether two tag responses belong to the same RFID tag. From Figure 6.2, we see that the RFID tag has two pieces of information that remains constant, the tag id and tag secret s. However, each time the tag replies to a query, the tag will select a different random number, nt, and thus, the resulting h(s,nr,nt) XOR id will always be different for every response. This prevents any illicit tracking, since the adversary is unable to determine whether two responses are from the same RFID tag or not. This defense remains valid even if the adversary can select its own nr value.

The third key requirement is to prevent or detect skimming. The adversary launching a skimming attack will observing the responses of a real RFID tag in attempt to create a fake tag that can pass off as a real tag. In the basic protocol, the adversary is able to observe the return value of nt, h(s,nr,nt) XOR id, However, it is unable to learn s or id based on the response. The adversary thus can only store h(s,nr,nt) XOR id directly into a fake RFID tag. This skimming attack will be detected when a legitimate reader queries the RFID tag. The legitimate reader will issue its own random number, which we denote as nr' to distinguish from the earlier nr observed by the adversary. Since the fake tag does not know s or id, the fake tag can only return h(s,nr,nt) XOR id, and not the correct h(s,nr',nt) XOR id.Since the backend server will attempt to test using nr' and not nr, this leads the backend server unable to find a correct (s,id) pair. Thus the skimming attack is detected.

III. CONCLUSION

In this paper, we have proposed an authentication protocol with provable security. Beyond the key RFID security requirements, there are some other RFID security requirements. This section discusses some protocols that address these requirements. Note that the protocols presented here may not necessary meet all the key security requirements because here advance protocols are generally designed to address specific issues or applications.

IV. REFERENCES

[1]. S. W. Wang, W. H. Chen, C. S. Ong, L. Liu and Y.W. Chuang, RFID application in hospitals: A case study on a demonstration RFID project in a taiwan hospital, system sciences, HICSS'06, Proceedings of the 39th Annual Hawaii International Conference 8 (2006).

[2]. R. Das, RFID forecasts, players & opportunities 2007–2017, Enterprise Networks & Servers, (March 2007).

[3]. C.F. Hernández, P.H. Ibargüengoytia-González, J.G. Hernández, J.A. Díaz, "Wireless Sensor Networks and Applications: a Survey", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, Pages 264 -273. March 2007.

[4]. Hasan Tahir, Syed Asim Ali Shah, "Wireless Sensor Networks– A Security Perspective", 12th IEEE International Multitopic Conference, Karachi, pp. 189-193, December 23-24, 2008.

[5]. Yee Wei Law, Paul J.M. Havinga, "How to secure a wireless sensor network", Published in Intelligent Sensors, Sensor Networks andInformation Processing 2005. IEEE pp 89-95.