Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-5, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

A Survey of Security in RFID Devices & Applications

Reeta Kumari Ashok Singh[1] & Prof. Deepti Dave[2]
[1,2]Department of Computer Science & Engineering, Bhopal, India

Abstract*: Security of statistics is a major issue in RFID situation as RFID is a wireless Radio frequency devices used in the wireless system. The data reads by the tag is send to reader which is then stowed at the server, but safety is a significant anxiety through the transmission of statistics from tag to reader. Though there are numerous security and verification methods implemented for the security of data and for the authentication of tag and reader. The existing technique offerings original sensing-enabled ramparts to unapproved interpretation and relay bouts against RFID systems without requiring any variations to the traditional RFID usage model. Here in this paper a review of all the prevailing technique are analyzed and discussed here.*

Index Terms **— RFID, AIDS, EPC, Eavesdropping, Tag, Reader.**

1. Introduction

Recently Radio Frequency Identification (RFID) schemes are the system where two parties communicate to each other via specified range of radio frequency especially in wireless sensor networks. During these days use of RFID system have been becoming more popular and aiming to be efficiently applied in many areas like library, banking as well as logistics and military etc. Some big corporations who have used this technology are Wal-Mart, Procter and Gamble, and the United State Department of Defense etc. We can say that RFID is a replacement of barcode technique. The Outdated bar-coding knowledge delivers an inexpensive answer for Automatic Identification Data Collection (AIDC) in industry applications but this technology has a main limitation where each of the barcoded article has to be skimmed separately, thus preventive the perusing speed[x]. In RFID system item or object does not required any line- of- sight operation and physical contact like barcode technology. The first recognized request of RFID was the "friend or foe" empathy organization used in combatant planes in World War II. After a few decades, RFID technology gained the courtesy since of its characteristic competence of existence used as a spare for bar codes in source chain and inventory management.

RFID Tag- A programmable RFID tag which consist

Figure 1 RFID Tag

RFID Reader- A antenna system to interrogate the RFID Tag.

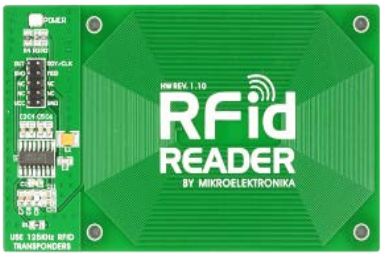

Figure 2 RFID Reader

RFID Middleware- RFID middleware is software that supports the communication between RFID readers and initiative organizations. It collects, filters, aggregates and applies business rules on data received from readers. It is also accountable for providing organization and nursing functionality to safeguard that the readers are associated, functioning properly, and are organized the accurate technique. It can contain a statistics supply for archival of read events[y]. There is an EPC global Reader Protocol 1.0 through which computers and readers may communicate with each. Here are also numerous middleware are available. For each middleware vendor must provide firmware for all supported readers. Middleware can be accomplished over user-friendly borders, like a standard software application. Also, middleware fluctuates in its

application style and middleware may be implemented on a host computer, a central server, or on intelligent readers.

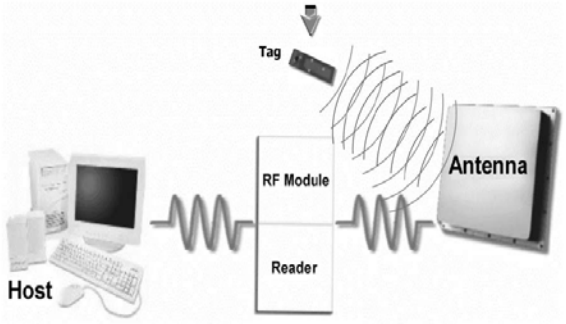

Figure 3 RFID working scenario

RFID Security Issues

One of the major difficulties to the acceptance of RFID technology is the lack of security and privacy. Since it contains small security on the RFID tags or during the communication with reader which causes the RFID system susceptible to many sorts of bouts e.g. information leakage, replay, and denial of service. There are some security issues are disused below.

1. Security of the tag, reader and the server: In this system the security of tag, reader and server is necessary.
2. Security of data in wireless network: In RFID data travel in a wireless network so the security of statistics is a significant factor to achieve better Communication and better efficiency of the data in the network and there should be very good security protocols to save the data in wireless network.
3. Security of unique data stowed at the receiver: The innovative statistics from the tag get stored at the server, and it is possible that the server can be retrieved in an unauthorized manner and also the server can get damage so the data will get lost so it also need fault tolerance.
4. Chances of eavesdropping: The safety of the statistics from tag to reader should be authenticated so that the chance of eavesdropping has been reduced.
5. Proper synchronization between tag and the reader: It is the flow of control from tag to the reader. The data moved from tag to the reader should be coordinated so that the data can't be lost and the chance of congestion has been reduced.
6. Proper Authentication: The system needs very strong way of authentication because no chance to access the private data by any unauthorized party.

2. Literature Survey

In 2011 [1] Tuan Anh Pham, Mohammad S. Hasan and Hongnian YuIn [1] offers the mutual verification procedure based on the encounter retort classical. The Advanced Encryption Standard (AES) is used as a cryptographic primitive to secure the data. It is a shared authentication procedure which utilizes AES-128 as a primitive to encrypt the communications communicated on the station. With that cipher chunk, the procedure can defend against many kinds of bouts including leakage attacks as well as tracking of tag attack.

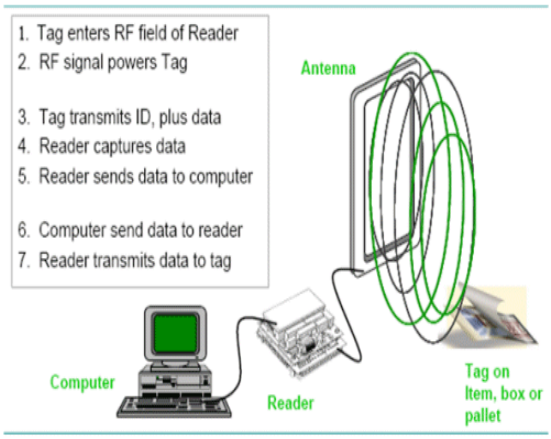

Figure 4. Basic Working Principle

In 2011 [2] Liangmin WANG, Xiaoluo YI, implies enhanced procedure simply uses CRC and PRNG processes maintained by Gen-2 that necessitate very low communiqué and calculation masses. They also progress two approaches based on BAN logic and AVISTA to demonstrate the safety of RFID protocol. BAN judgment is used to give the resistant of etiquette precision, and AVISTA is used to affirm the authentication and secrecy properties.

In 2008 [3] Tieyan Li analyze the security susceptibilities of a domestic of ultra-lightweight RFID shared authentication procedures: LMAP [4], M2AP [5] and EMAP [6], which are proposed by Peris-Lopez et al. Here they identify various attacks such as de-synchronization as well as disclosure attack. The implemented technique enduringly incapacitates the verification competence of a RFID tag by abolishing harmonization amongst the tag and the RFID reader. Indeed, notice that the key idea employed in the identity disclosure attack.

In 2006 [7] H. Lee, J. Yang, and K. Kim proposed the SASI was openly planned in as an upgrading of the UMAP procedures, in instruction to provide authenticity and integrity and withstand all the possible attacks the UMAP

protocols are subject to. The structures of these protocols are pretty much similar (see [8], [9], [10]). We have examined SASI and we have displayed that the etiquette offerings vulnerabilities which can be easily used by an adversary who can interact with the Tag. All that is needed is an illegal Reader which can enquiry the Tag and get replies.

In 2003 [11] Weis, Sarma, Rivest and Engels future the use of hash-locks in RFID strategies. A first method, called Deterministic hash tresses, was obtainable in. A tag is typically in a \locked" state pending it is enquired by a reader with a precise provisional meta identifier Id. This is the result of chopping an accidental worth (nonce) designated by the reader and stowed into the tag. Readers are then used to provisions the Id and the nonce in order to be bright to interrelate with the tag. The reader can solve a tag by distribution the nonce worth. When a tag obtains it, the worth is checkered.

In 2004 [12] Ohkubo, Suzuki and Kinoshita (OSK) proposed the OSK protocol. Its purpose is to guarantee the lawful response of the tag smooth under an vigorous attack. In this arrangement each tag is primed with a underground value xi and two unidirectional functions h1 and h2. When a tag obtains a demand from a reader, it apprises the price xi with the novel worth obtained from the computation of ht 1(xi) [11]. The tag cataloguing mostly grounded on which were the processes functional on-chip. These tags of high storage are alienated into two lessons: “full-fledged” and “simple”. Full-fledged tags support aboard conservative cryptography like symmetric encryption and cryptographic one-way functions.

In 2006 [13] Tsudik proposed YA-TRAP (Yet-Another Trivial RFID Authentication Protocol).This procedure describes a method for the cheap untraceable empathy of RFID tags. YA-TRAP includes trifling communication among devices and a low computational weight on the back-end server. With these features, this scheme is attractive for applications where the information is processed in data groups [11].

In 2007 [14] Chien and Chen (CC) a shared confirmation procedure for RFID conforming to the EPC Class 1 Generation 2 standards was introduced by [15]. A challenge-response protocol is used to prevent replay attacks. The server database maintains copies of both old and new tag keys to resist DoS attacks. Both the verification important and the admission key are efficient after a positive session in order to give backward untraceability.

In 2005 [16] Dimitriou’s scheme (D) is an RFID authentication protocol that enforces user privacy and protects against tag cloning. However, amongst valid meetings, the tag identifier remnants the identical, thereby manufacture the arrangement susceptible to tracking. Additionally, the scheme is prone to DoS attacks.

In 2006 [17] Lim and Kwon (LK) describe an RFID authentication scheme sustaining both advancing and retrograde untraceability and enabling perfect ownership transfer. They define update as deterministic evolution (of stored secrets) and refresh as probabilistic evolution, where the refresh process is introduced to help provide forward untraceability. A tag and a server both refresh their secrets using exchanged random numbers if an authentication procedure completes successfully [7]. If an authentication procedure fails, the tag updates its secrets (i.e. using a deterministic process). These techniques make the scheme partially secure against server impersonation.

In 2005 [18] Ohkubo, Suzki, and Kinoshita (OSK) propose an RFID privacy protection scheme providing indistinguishability (i.e. a tag output is indistinguishable from a truly random value and unlinkable to the ID of the tag) and backward untraceability. This scheme uses a low-cost confusion hawser instrument to update tag secret information to provide these two security properties. However, it is subject to replay attacks [15], and hence it permits an adversary to impersonate a tag without knowing the tag secrets.

3. Problems in Existing System

1. **Security of the tag and the reader as well as the server:** As the data from tag moves to the reader, security has to be maintained during the flow of data. Hence the security is maintained at the tag and the reader for the better efficiency of the data. since we are using authentication techniques hence the chances of accessing tag or reader as well as server gets difficult.
2. **The original data stored at the receiver side:** The original data from the tag is readed by the reader and is stored at the server, if the server can be retrieved in an illegal method and if the server indemnities the statistics will be lost, hence chances of fault tolerance.
3. **Chances of eavesdropping:** The protocols that are implemented for the security of the data from tag to reader should be authenticated so that the chance of eavesdropping has been reduced.
4. **Synchronization between tag and the reader:** Synchronization between the tag and the reader is the flow of control from tag to the reader. The

data moved from tag to the reader should be synchronized such that the data can't be lost and the chance of congestion has been reduced.

4. Conclusion

The Radio Frequency Identification is a process of sending data using Radio waves over wireless channel. Hence various techniques are implemented for the security of these data. Here in this paper a survey of all the techniques implemented for the security is analyzed and compared here so that on the basis of their various advantages and limitations a new and efficient technique is implemented in future.

5. References

[1] Tuan Anh Pham, Mohammad S. Hasan and Hongnian Yu, "A RFID mutual authentication protocol based on AES algorithm", 2012 UKACC International Conference on Control, pp. 997 – 1002, Sept. 2012.

[2] Liangmin Wang, Xiaoluo YI, Chao LV, Yuanbo Guo "Security Improvement in authentication Protocol for Gen-2 Based RFID System". School of Computer Science and Communication Engineering, Jiangsu University, doi:10.4156/jcit.vol6. Issue 1.18. 450004, China.

[3] Tieyan Li, "Security Analysis on a Family of Ultra-Lightweight RFID Authentication Protocols", Institute for Info-comm Research (I2R), 21 Heng Mui Keng Terrace, Singapore 119613.

[4] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez- Tapiador, and A. Ribagorda. LMAP: "A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags." In: Proc. of 2nd Workshop on RFID Security, July 2006.

[5] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez- Tapiador, and A. Ribagorda. "M2AP: A Minimalist Mutual- Authentication Protocol for Low-cost RFID Tags". In: Proc. of International Conference on Ubiquitous Intelligence and Computing UIC'06, LNCS 4159, pp. 912-923. Springer- Verlag, 2006.

[6] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez- Tapiador, and A. Ribagorda. "EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags". In: OTM Federated Conferences and Workshop: IS Workshop, November 2006.

[7] H. Lee, J. Yang, and K. Kim. "Enhanced mutual authentication protocol for low-cost RFID." White Paper Wp-Hardware-031, Auto-ID Labs, 2006.

[8] Hung-Yu Chien, "SASI: A New Ultra lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions On Dependable And Secure Computing, Vol. 4, No. 4, October-December 2007.

[9] Soichi Kubota, Yoshiharu Okamoto, Hideo Oda "A Study of the Security on Driving Safety Support System using RFID", 7th International Conference on ITS Telecommunications, pp. 1 - 4 , 2007.

[10] Wen-Her Yang, and Hun-Min Sun, "An Authentication Protocol without Trusted Third Party", IEEE Communications Letters, Vol. 1, No. 3, May 1997.

[11] Aragones-Vilella, A. Martinez-Balleste and A. Solana's "A Brief Survey on RFID Privacy and Security "J. Crises Reserch Group Unesco Chair in Data Privacy Dept. of Computer Engineering and Mathematics, Rovira I Virgili University.

[12] M. Ohkubo,K. Suzuki, and S. Kinoshita. "Efficient hash chain based RFID privacy protection scheme". In International Con- ference on Ubiquitous Computing - Ubicomp, Workshop Privacy: Current Status and Future Directions, 2004.

[13] G. Tsudik. YA-TRAP: "Yet another trivial RFID authentication protocol". In Fourth annual IEEE International Conference on Pervasive Computing and Communications Work- shops (PERCOMW'06), pages 640-643, 2006.

[14] H. Chien and C. Chen. "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards". Computer Standards & Interfaces, 29(2):254–259, February 2007.

[15] H. Chien and C. Chen. "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards". Computer Standards & Interfaces, 29(2):254–259, February 2007.

[16] T. Dimitriou. "A lightweight RFID protocol to protect against traceability and cloning attacks". In Conference on Security and Privacy for Emerging Areas in Communication Networks — Secure Comm., IEEE, pages 59–66, Athens, Greece, September 2005.

[17] C. Lim and T. Kwon. "Strong and robust RFID authentication enabling perfect ownership transfer". In P. Ning, S. Qing, and N. Li, editors, Conference on Information and Communications Security — ICICS '06, volume 4307 of Lecture Notes in Computer Science, Springer-Verlag ,pages 1–20, Raleigh, North Carolina, USA, December 2006.

[18] Ohkubo, Suzki, and Kinoshita "RFID Privacy Issues and Technical Challenges" Communications of the ACM - Special issue: RFID, Vol. 48, No. 9, pp. 66 – 71, 2005.

•