A Bi-direction Authentication Protocol for RFID Based on the Variable Update in IOT[†]

Liu Yang^{1,2*}, Peng Yu², Wang Bailing¹, Qu Yun¹, Yuan Xinling¹, Yin zelong¹

Department of Computer Science & Technology Harbin Institute of Technology at Weihai, Shandong, China Automatic Test and Control Institute Harbin Institute of Technology, Harbin, China Liuyang322@hit.edu.cn

Abstract. With the development and wide application of RFID technology in the Internet of Things, RFID system for user privacy protection and information security requirements have become increasingly prominent. In this paper, the RFID system security requirements and the existing lack of security authentication protocol RFID Bi-direction authentication protocol based on variable update. Hash function characteristics, mutual authentication in RFID systems, effectively preventing the counterfeiting phenomenon within the system, while using the system initial value cycle update, enhance the level of security certification to overcome a variety of security attacks. The agreement has certain advantages in safety performance and the complexity of the algorithm, a high level of security and practicality

Keywords: Bi-directional authentication, Hash, RFID, IOT

1 Introduction

With the widely application of RFID technology, the security of the RFID system is increasingly prominent. The communication between RFID tag and Reader adopts wireless communication, which is considered unsafe and easily attacked by various ways[2]. especially on security and privacy protection which has seriously hindered the further development of RFID technology and to be a key problem effecting RFID system.

For the security requirement of different RFID tags, many solutions have been proposed at present. These solutions are divided into two kinds of mechanisms[3]: physical mechanism and password system. Physical mechanism is mainly for the RFID tag which is not suitable for the executive password operation or one-time tag, including Kill command mechanism[4], active jamming[5], Blocker Tag[6], Ferrari cage[7] and so on. Although these physical mechanisms could partly ensure the safety of the RFID signal, these methods which are limited used need extra physical equipment and increase the RFID system cost. Therefore, the industry more inclines

[†] Supported by the National Science Nature Foundation of China under Grant No 61170262

to password mechanism. Password system mainly takes the method of the bidirectional authentication between tag and Reader to control the access to the tag, which enhance the security and privacy of the RFID system. More typical security protocols: Hash-lock protocol, randomizing Hash-lock protocol, hash chain protocol, ID change protocol based on Hash, distributed challenge-response protocol and so on[8].

We have summarized the problem about RFID security in the environment of IOT and propose RFID secure authenticated protocol based matrix variable update. The protocol ensures the privacy of information realizes three party bi-directional authentications, solves the problem that the existing RFID secure authenticated protocol couldn't realize bi-directional authentication in tag, Reader and Backend database, effectively resists attacks from internal system, updates and deals with initial variables periodically and improve the security of RFID system. Compared with the existing RFID secure authenticated protocol, ours could prevent existing security attacks and it has certain advantages on computational complexity and time complexity. Meanwhile, it has the high safety and practicality.

2 Design of Security Authentication Protocol

In this section, we describe our algorithm for detecting sensors whose readings (measurements) are faulty. Firstly, we illustrate NDHN by using an aggregation session scenario example, and then we present the detection procedure and the algorithm.

2.1 System Initialization Process

- 1) Information stored in the database (DB): the reader ID $(R_1,R_2..R_n)$, the initial value of each reader R_1 (X_1,Y_1) $..R_n(X_n,Y_n)$; System initial value (X,Y); Tag information and tag ID $(T1,T2,\cdots Tid)$; Session key K.
- 2) Information stored in the reader (R): the reader ID (R_n) , the initial value of the reader $R_n(X_n,Y_n)$ System initial value (X); the value of Hash(y'||Tid') calculated previously; Session key K.
 - 3) Information stored in tag T: System initial value (X,Y); Tag Tid.

2.2 Authentication process

- 1) The reader R generates a random number Rr1, calculates Hash (X||Rr1) and sends request and Hash (X||Rr1)||Rr1 to the tag T.
- 2) The tag T calculates $\operatorname{Hash}(X'\|Rr1)$ compared with the $\operatorname{Hash}(X\|Rr1)$ received after receiving information. If the $\operatorname{Hash}(X'\|Rr1)$ calculated is equal to the one received, the authentication for the reader R would be accomplished. If the $\operatorname{Hash}(X'\|Rr1)$ calculated isn't equal to the one received, the message would be gave up. The tag T calculates $\operatorname{Hash}(Y'\|Tid')$ $\|\operatorname{Hash}(X'\|Rr1\|Tr1)$ $\|Tr1$ and sends it.

- 3) The reader R judges whether the $Hash(Y'\|Tid')$ stored is equal to the $Hash(Y'\|Tid')$ after receiving information. The equality of them shows that being queried and stop querying, which prevents the attacker from making DDos attack on the server with repeatedly sending query information. If they aren't equal, the reader calculates $Hash(X'\|Rr1)$ compared with the $Hash(X\|Rr1)$ received. If the $Hash(X'\|Rr1)$ calculated is equal to the one received, the authentication for the tag T would be accomplished. At the same time, the reader R calculates $Hash(Y'\oplus Tid')\|Hash(Y_n\|Rr2\|Rid)\|Rr2\|Tr1$ and sends it to the database DB.
- 4) The database DB calculates $Hash(Y'_n||Rr2||Rid)$ compared with the $Hash(Y_n||Rr2 \oplus Rid)$ received after receiving information and gets Rid and (X_n, Y_n) to accomplish the authentication for the reader R. If the Hash(Y||Tid) calculated is equal to the one received and Tid has been obtained, the authentication for the tag T would be accomplished. The database DB consults with the reader R about the session key K through a secure channel and calculates $K+(Tid||Rr2||X_n)||Hash(Y||Tid||Tr1)$ and sends it to the reader R.
- 5) The reader R uses the session key K to calculate K- $(K+ (Tid||Rr2||X_n))$ for obtaining the ID of the tag T (Tid)after receiving information and accomplishs the authentication for the database DB. After that, R sends the Hash(Y||Tid||Tr1)calculated to the Tag T.
- 6) The tag T calculates Hash(Y||Tid'||Tr1) compared with the Hash(Y||Tid||Tr1) received. If the Hash(Y||Tid'||Tr1) calculated is equal to the one received, the authentication for the database DB would be accomplished.

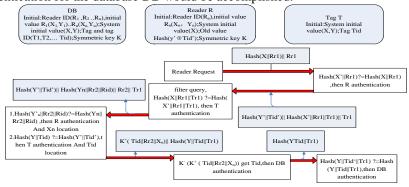


Fig. 1. RFID bi-directional authentication

3 Analysis of the Protocol's Performance

RFID security mainly reflects in the privacy of users and the security of information. The authentication scheme could effectively defend against various attacks in IOT.

RFID security protocol not only guarantees privacy and security of information transmission but also synthetically considers the inherent characteristic of the tag and the reader. The characteristic is mainly on the limitation of computational power and memory capacity, which lowers the cost of RFID system. Most protocols all have n

order of magnitudes operation and a part of protocols involve several n order of magnitudes operations, which results in the phenomenon that arithmetic speed is slower and nodes consume more energy. The protocol allows the strong computing power database to deal with a number of calculations and its calculation load is lighter than other protocols. Although the calculation load involved in the tag and the reader is a little heavier than other algorithms, it is able to meet the safety need of RFID system overall.

4 Conclusion

The article has analyzed RFID security issues in IOT. We propose the RFID Two-way authentication protocol based on updating variables and securely transmit ID in ciphertext form between the reader and the tag through Hash function characteristic on purpose to guarantee the privacy of information. Meanwhile, we realize three party mutual authentications and solve the problem that RFID security certificate couldn't realize in the tag, the reader and the database so that the internal system counterfeit phenomenon is defended effectively. At the same time, we adopt the method to periodically update system initial value in order to enhance security level and overcome various security attacks. Compared with the existing secure authentication protocols and computational complexity, the protocol has a certain advantage on algorithm complexity and safety performance and it has a higher security and practical applicability

References

- 1. Gilbert H, Matthew R, Sibert H .An active attack against HB+: A provably secure lightweight authentication protocol.IEEElectronics Letters, 2005, 41(21):1169-1170.
- BURMESTER M.secure ubiquitous systems: Universally composable RFID authentication protocols.Proceedings of the 2th International Conference on Security and Privacy in Networks.2006.176-186
- 3. Sarma.A, Girao. J. Identities in the Future Internet of Things. In: Wireless Personal Communications, Springer Netherlands, 2009(49):258-263
- 4. ZHANG F,SUN X.A universally composable secure RFID communication protocol in supply chains[J]. Chinese Journal of Computers, 2008, 31(10):1754-1767.
- 5. ZHOU Y B,FENG D G. Design and analysis of cryptographic protocols for RFID[J]. Chinese Journal of Computers, 2006, 29(4):581-589.
- 6. MOLNAR D.A scalable delegatable pseudonym protocol enabling ownership transfer of RFID tags. Workshop on Selected Areas in Cryptography.2006.276-290.
- 7. Letri V, Medeirosde B. Universally composable and forward secure RFID authentication and authenticated key exchange. Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2007.242-252.
- 8. KIM H S.The design and verification of RFID authentication protocol for ubiquitous computing. Proceedings of the 18Th International Workshop on Database and Expert Systems Applications. 2007.693-697.