# Research on Defense Technology of Relay Attacks in RFID systems

Weiwei Shen[1,2], He Xu[1,2], Rui Sun[3] and Ruchuan Wang[1,2]

[1] College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[2]Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing, 210003, China
[3]College of Overseas education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
Email: 1214042932@njupt.edu.cn; xuhe@njupt.edu.cn, rsun03@nyit.edu, wangrc@njupt.edu.cn

***Abstract*** —Relay attack is the most menacing attack that radio frequency identification technology (RFID) systems are facing currently. An attacker could use limited resources to build up this kind of attack with the encryption algorithm which is difficult to detect out. At present, the main methods to resist the relay attack in RFID system include measuring the received signal strength (RSS) between the reader and the tag, the round-trip time (RTT) of the signal and introducing a second channel - Environmental Conditions. Most of the studies nowadays are adopted the distance bounding protocols which can resist the relay attack by measuring the round-trip time of the short authentication messages between the tag and reader. Many of these protocols have been proposed, such as Hancke and Kuhn's(HK) protocol, Munilla, Ortiz and Peinado's (MOP) protocol and so on. In recent years, researchers have put forward a brand-new solution of using the second channel - environmental conditions to resist relay attack, such as using button, noise, temperature, etc. This paper mainly does research on the defense techniques for relay attacks in the RFID system and gives some introductions and summaries of the domestic and foreign relevant situation against such attacks.

***Index Terms—***relay attack; RFID systems; distance bounding protocol; based on the button; noise

## I. Introduction

In today's world, radio frequency identification technology (RFID) has been widely used in many fields, for example, management of supply chain[1], electronic passports[2], credit cards[3], driving license[4], vehicle system (electronic toll collection system)[5], Access control card system[6] (parking lot, buildings, public transportation), location service[7] as well as medical and other fields. It is necessary to control the cost of a single RFID tag for the big amount usage which leads to the weak ability of one RFID tag and can not support complex cryptography computing as well. In August 2008, three students at the Massachusetts institute of technology announced that they have successfully cracked the Boston Metro Card. Since then, those kinds of cracking attack events are continuously exposed in recent years. The potential safety hazard that the RFID system at present mainly includes the following categories: eavesdropping, man-in-the-middle attack, deception, cloning, replay, physical crack, tampering with information, denial of service attacks and RFID virus, etc. For the past few years, it comes out a new attack called relay attack which belongs to the man-in-the-middle attack. This kind of attack is easy to set up, needs less resources and is also difficult to detect.

In 2006, Hancke [8]implemented the earliest relay attack which used Ultra High Frequency (UHF) antenna to connect the attack equipment and complete analog data forwarding. In 2010, Weiss [9] also got the similar results by using Near Field Communication (NFC) mobile equipment. In fact, two Nokia mobile phones which support NFC have been able to implement relay attack in P2P communication mode or reader/tag mode [10-12]. Desmedt et al., applied such attacks to the communication protocol for the first time [13]. Right now, solutions to solve delay attacks can be divided into two aspects, whether in China or abroad. One is distance bounding protocol and the other is introducing a second channel - Environmental Conditions. The research of distance bounding protocol belongs to theoretical level and two protocols referred in document [14, 15] have accomplished already. In China, researches related to relay attacks are still not many actually, especially in its defense mechanism.

## II. Related concepts of relay attacks

### A. Definition of Relay Attacks

The concept of relay attack was derived from the chess grand master problem in cryptography at the earliest [16]. Problem description: two chessboards A and B, each side chessboard seated a chess grand master AM and BM. A newbie can at least defeat one of the masters or end in a draw through repeating steps of AM and BM.

In real relay attack situation, the attacker needs to simulate an illegal reader VR and an illegal tag VT and builds up a high-quality and low-latency relay link

This work was supported by the Natural Science Foundation of Jiangsu Province, China(Grant No. BK20140886, No. BK20140888), China Postdoctoral Science Foundation(Grant No. 2014M561696, No. 2014M551636), Natural Science Foundation of the Jiangsu Higher Education Institutions of China(Grant No. 14KJB520030), Jiangsu Planned Projects for Postdoctoral Research Funds(Grant No. 1401005B, No. 1302090B) and NUPTSF（Grant No. NY213034, No. NY214060 and No. NY214061）

Corresponding author email: xuhe@njupt.edu.cn.

between two legal users R and T. VR is placed near the victim T and VT is placed near the victim R. The attacker can forward the messages of two legal users intactly through the relay link. As shown in Fig.1, it is a relay attack scenario:

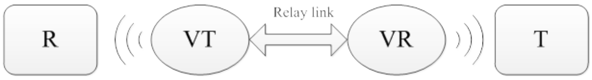

Fig.1. relay attack model

Relay attack has two types. One is mafia fraud attack and the other is terrorist fraud attack. Mafia fraud attack: Desmedt was the first one who described the mafia fraud attack [17]. Terrorist fraud attack is an extension of mafia fraud attack. (as shown in Fig.3)

According to the existing literature research, this paper divides the protection techniques of delay attacks at present into two parts. (a) distance bounding protocol which combined with characteristics of physical layer and mechanisms of Cryptography[18,20-25] (b)Introduce the second channel - environmental conditions[19, 26, 27]. This paper will compare and analyze these two kinds of techniques.

### B. *Distance Bounding Protocol*

In relay attack, the legal Reader (R) would trust the legal tags (T) are in the legal range by forwarding messages between R and illegal tags(out-of-field Tag). Distance bounding protocol is the most efficient way to resist delay attack and this kind of protocol measure the signal intensity and round-trip time between tags and readers. However, this method based on the signal intensity is unsafe since the adversary can easily magnify the signal intensity or use stronger signal intensity. Therefore, most of the distance bounding protocols are focused on measuring the RTT of the short authentication messages.

### C. *Second Channel - Environmental Conditions*

The main efficient way to defense relay attack is using RTT to measure the physical distance between Reader and Tag. However, this method is hard to completely defense the attacker with high bit rate network or victims in near field.

In 2014, Sukin Kang et al. put forward another method that is introducing a second channel apart from the communication channel such as a screen equipment, Global Positioning System (GPS), noise, temperature, or an accelerometer [26]. The second channel can not be delayed and exits in the real world. This kind of channel must be random. For instance, surrounding noise is a kind of typical random data.

## III. COMMON DISTANCE BOUNDING PROTOCOLS

### A. *Hancke and Kuhn's(HK) Protocol*

According to measuring the round-trip time of the switching messages, Desmedt et al introduced the concept of distance bounding [28, 29].In 2005, Hancke and Kuhn came up with the first distance bounding protocol based on the framework of the RFID[18]. Then this protocol had been applied widely and a great many protocols made it as a reference protocol. The attacker just have 3/4 of the probability of getting the right reply. In n times rounds, the success probability for attackers is$(\frac{3}{4})^n$.

### B. *Munilla, Ortiz and Peinado's (MOP) Protocol*

In 2006, Munila and Peinado put forward MOP protocol[20, 21]. This protocol is the variant of HK protocol which introduces the concept of empty challenge based on HK. Empty challenge means reader doesn’t send out bits. The basic concept is that challenge can be zero, one or void (don’t send any data bits). Mop protocol is aimed at reducing the attackers’ success probability without using any extra signal messages. Nevertheless, the disadvantages are need of three physical states 0, 1 and void. This is very hard to implement. In addition, attackers’ success probability is higher than （1/2)$^n$.

### C. *Reid et al. Protocol*

In 2007, Reid et al first put forward the distance bounding protocol based on symmetric key which can be executed in low cost devices[30]. It has been solved the disadvantages that HK protocol is easily suffering from terrorist fraud attack. It is an enhanced edition of HK protocol. Compared with HK protocol, its efficiency is the same and the main difference is adding a symmetrical encryption ( XOR operation). In 2010, Mitrokotsa et al. in literature[31] proved this protocol can resist mafia fraud attack up to $(3/4)^n$ probability which drops down with the increase of the noise.

### D. *Tu and Piramuthu's (TP) Protocol*

In 2007, in order to reduce the attackers’ success probability, Tu and Piramuthu[24] used four for-loop loops in fast switching bits stage. After switching n/4 data bits, reader will send out different hash values. For four different combination values, they repeat four times in for outer loop.In each outer loop, inner loop repeats n/4 times. Inner loop is a fast bits switch, that is reader send random bit $q_i$ then tags reply $C_i$ . This protocol makes the success probability for attackers up to (9/16)$^n$ which uses to defense terrorist fraud attack. However, this protocol is useless for common active attacks.

### *E.* Kim and Avoine's( KA) Protocol

In 2009, Avoine et al. put forward KA protocol[23]. In order to overcome the disadvantages of MOP protocol, they introduced mixed challenge on the basis of MOP protocol. That is reader send data bits to tags in fast bits switching stage can be divided into two parts. One is random challenge bits and the other is predefined challenge bits. Also, both reader and tags can know all the challenge bits previously. this protocol can not use any confirmation information compared with MOP protocol. It improved the efficiency in computer science and telecommunication greatly.

### F. *Comparison With Distance Bounding Protocols*

Attackers have two main attacking methods. One is query ahead of time which exists risks of being detecting out by tags. The other one is do not query tags ahead and try to guess the response bits of the tags. The success probability of the attackers depends on which represents the probability that full challenge(all challenge bits except void state) will happen. TABLE I referred that the success probability means adopting query ahead situation. Distance bounding protocol needs to take using lower calculation resources( memory and time) into consideration. Balance the probability and complexity, probability and memory, mafia fraud attack and terrorist fraud attack to find a compromised scheme. From[32], when $p_f = \frac{4}{5}$, the success probability of attackers will be the lowest. So the best attack probability is $(\frac{9}{16})^n$ nowadays(like: TP protocol). So the least memory consumption is 2n and the most memory consumption is 4n in KA protocol but the mixed challenge idea is worth applying. TP protocol is a distance bounding can both defense mafia fraud attack and terrorist fraud attack but can not deal with common active attacks.

TABLE I:COMPARISON WITH DISTANCE BOUNDING PROTOCOLS

| protocol | memory | mafia fraud attack | Attack success probability | terrorist fraud attack | advantages | disadvantages |
|---|---|---|---|---|---|---|
| HK | 2n | yes | $(\frac{3}{4})^n$ | no | small demand for memory | High success attack probability; one-way authentication protocol; waste n places memory |
| MOP | 3n | yes | $(\frac{1}{2})^n$ | no | Low success attack probability | Add n bits memory; waste n places memory; empty challenge is difficult to operate |
| Reid et al. | 2n | yes | $(\frac{3}{4})^n$ | yes | Low demand for memory; can defense terrorist fraud attack | Low demand for memory |
| TP | 2n | yes | $(\frac{9}{16})^n$ | yes | Low demand for memory; low success attack probability; can defense terrorist fraud attack | Can not deal with active attacks well |
| KA | 4n | yes | $\frac{1}{4}\sum_{i=1}^{i=n}(\frac{5}{8})^{i-1}(\frac{1}{2})^{n-i+1}$ | no | bidirectional authentication | Consume a lot of tags' memory; wrong calculation method to probability |

## IV. INTRODUCTION OF THE SECOND CHANNEL:ENVIRONMENTAL CONDITIONS

### A. *Method Based On Buttons*

Kang et al. have put forward a method based on button to defense relay attacks[26] which uses a button to provide a basic interface. Most of the devices have at least one button for setting the devices or manual operation. Before starting authentication stage, the user needs to press two devices P and V at the same time. Each device measures the button pressing or button releasing time. P sends measured time Tp to V. V decides whether it is a legal user by Tp and Tv. If the difference between Tp and Tv is lower than predefined critical value, V will accept P. Otherwise, reject.

### B. *Relay Attacks Based On Noise Statistical Change Detection*

In 2013, Hamida et al. has put up the new method of relay attack in the RFID system[19], using the physical layer characteristics. When a relay communication happens, examine the change of the noise. Assume attackers can be added up to wireless communication link, an amplifier could reduce the path loss and the distance-decay effect. In addition, the filter is used to eliminate the random noise which may affect the signal.

Emitter A sends signal $x_A$ to receiver B. B acts as a delay attack detector. B receives signal $y_B$ . By filtration, B measures and extract noise then saves as different noise samples. It can estimate the variance $\hat{\sigma}_B^2$. B uses Fisher hypothesis test[23]to calculate a judging threshold $\gamma$ to detect delay attack. Node B extract noise and estimate the variance of the noise $\hat{\sigma}_t^2$ when it receives messages sent by A. Then comparing variance of the noise $\hat{\sigma}_t^2$ and $\hat{\sigma}_B^2$. The research illustrated that noise was greatly affected by relay attacks. Literature [12] has proved this conclusion. The information of the noise can be collected by available RF front-end equipment without extra hardware and no need to change the standard protocol. This case can be applied to sensor, adhoc network and RFID system, and no need of encryption methods. Moreover, the probability of detecting out delay attacks can be up to 0.97.

### *C. Method Based On Temperature Senors*

In 2013, Urien et al. put forward a mutual authentication protocol based on elliptic curve[27]. It is the first time to use the sensors' information of reader and tags to defense relay attacks. The mutual authentication protocol put forward by Urien which use: (a) temperature of the tags and (b)Round-trip time of the signal to measure the physical distance. This method uses a RFID tag with temperature sensor function, a reader with temperature sensor function. The measured temperature switch from reader and tag, then we detect the efficiency by difference of the temperature. If the physical distance is close, the difference should be small as well ( caused by measuring equipment).

At the beginning of the protocol, it mainly define a maximum permissible amount of variation $\varepsilon$ . If variation of the temperature $|T_R - T_T| > \varepsilon$ , both sides will terminate the protocol. Temperature measured by reader and tag L and R will be encrypt.The response of the tag based on the port of the reader $Z_R$ ( $Z_R = (L \oplus R \oplus x_R)$ ) and random numbers in tag port. Then tag chooses three different response values. Attackers use query ahead method to query repeatedly will be at most 1/3 success probability.

### *D. Comparison With Three Environmental Conditions(see in TALBE II)*

TABLE II:COMPARISON WITH THREE ENVIRONMENTAL CONDITIONS

| Environmental condition | Based on button | Based on noise | Based on tempera |
|---|---|---|---|
| theoretical basis | The time of the button pressing case can be measured | Variance of the noise, receiving signal to noise ratio | Distance bounding protocol |
| main idea | Detect out attackers according to predefined time threshold and time difference measured by legal users | Detect out attackers by noise variance ration $\frac{\hat{\sigma}_t^2}{\hat{\sigma}_B^2}$ and $\gamma$ | Take advantage of tag's temperature and RRT of the signal to measure the physical distance. Tag chooses three different response value. |
| advantages | Easy to implement and every mobile device needs at least equipped with one button | No need to modify the standard protocol and no need for encryption methods | Can defense terrorist fraud attacks |
| disadvantages | Unstable, hard to operate | complex calculation | Need extra hardware |

## V. CONCLUSIONS

Right now, systems applied in RFID wireless communications are all need to defense delay attack. For the independence of cryptography, we cannot solve those kind of attacks via simple cryptographic algorithms in application layer. Also, attacks occurred passively without the usage of label or the information of reader and that's the reason why it is difficult to defense. Currently, the main method is the distance bounding protocol to resist the relay attack in RFID system which use the round-trip time of messages to measure the physical distance between legal two sides. When choosing a distance bounding protocol, we need to take memory consumption, calculation complexity, success probability, whether can defense mafia fraud attack or terrorist fraud attack into consideration. Design a safe and proper distance bounding protocol is one of the most efficient way to defense RFID relay attack. However, when attackers use high speed network or just near the victims, this method is quite difficult to resist relay attack. Recent years, another solution has been put forward that introduce the second channel, which needs to choose a random data according to the environmental conditions. This solution need to balance on calculation complexity, cost of extra hardware, operationality, stability, etc. In actual RFID application system, we need to select a most suitable one method for usage.

## REFERENCES

[1] J. C. Chen, C. Cheng and P. B. Huang, "Supply chain management with lean production and RFID application: A case study," *Expert Systems with Applications*, vol. 40, no. 9, pp.

3389-3397, 2013.

[2] S. Kundra, A. Dureja and R. Bhatnagar, "The study of recent technologies used in E-passport system," in *2014 IEEE Global Humanitarian Technology Conference-South Asia Satellite (GHTC-SAS)*, 2014, pp. 141-146.

[3] Y. Zhu, H. Chen and K. H. Wang, "Consumer’s acceptance of high-tech products: the case of RFID credit cards in Taiwan," *International Journal of Technology Marketing,* vol. 9, no. 2, pp. 143-162, 2014.

[4] M. Agarwal, M. Sharma and B. Singh, "Smart ration card using RFID and GSM technique," in *2014 5th International Conference on Confluence the Next Generation Information Technology Summit (Confluence)*, 2014, pp. 485-489.

[5] P. Jagtap, P. Barge, S. More, and A. D. Gujar, "Toll Collection and Stolen Vehicle Detection Using RFID," *International Engineering Research Journal,* vol. 1, no. 2, pp. 36-39, 2015.

[6] Y. Shu, Y. J. Gu and J. Chen, "Dynamic authentication with sensory information for the access control systems," *IEEE Transactions on Parallel and Distributed Systems,* vol. 25, no. 2, pp. 427-436, 2014.

[7] A. Montaser and O. Moselhi, "RFID indoor location identification for construction projects," *Automation in Construction,* vol. 39, pp. 167-179, 2014.

[8] G, E, R, H, A, R, D, P, and H, "Practical Attacks on Proximity Identification Systems (Short Paper)," *IEEE Computer Society,* pp. 328-333, 2006.

[9] M. Weiß, "Performing relay attacks on iso 14443 contactless smart cards using nfc mobile equipment," *Master's Thesis, Munich,* 2010.

[10] Z. Wang, Z. Xu, W. Xin, and Z. Chen, "Implementation and analysis of a practical NFC relay attack example," in *Proceedings of the 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control*, 2012, pp. 143-146.

[11] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical NFC peer-to-peer relay attack using mobile phones," in *Radio Frequency Identification: Security and Privacy Issues*: Springer, 2010, pp. 35-49.

[12] L. Francis, G. P. Hancke, K. Mayes, and K. Markantonakis, "Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones.," *IACR Cryptology ePrint Archive,* vol. 2011, p. 618, 2011.

[13] Y. Desmedt, C. Goutier and S. Bengio, "Special uses and abuses of the Fiat-Shamir passport protocol," in *Advances in Cryptology—CRYPTO’87,* 1988, pp. 21-39.

[14] K. B. Rasmussen and S. Capkun, "Realization of RF Distance Bounding.," in *USENIX Security Symposium*, 2010, pp. 389-402.

[15] M. Kuhn, H. Luecken and N. O. Tippenhauer, "UWB impulse radio based distance bounding," in *Positioning Navigation and Communication (WPNC), 2010 7th Workshop on,* 2010, pp. 28-37.

[16] J. H. Conway, *On numbers and games* vol. 6: IMA, 1976.

[17] Y. Desmedt, "Major security problems with the 'unforgeable' (Feige)-Fiat-Shamir proofs of identity and how to overcome them," in *SecuriCom*, 1988, pp. 15-17.

[18] G. P. Hancke and M. G. Kuhn, "An RFID distance bounding protocol," in *Conference on Security and Privacy for Emerging Areas in Communications Networks SecureComm 2005*, IEEE,Athens,Greece, 2005, pp. 67-73.

[19] S. Hamida, P. Thevenon, J. Pierrot, O. Savry, and C. Castelluccia, "Detecting relay attacks in RFID systems using physical layer characteristics," in *Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP*, 2013, pp. 1-8.

[20] J. Munilla and A. Peinado, "Distance bounding protocols for RFID enhanced by using void‐challenges and analysis in noisy channels," *Wireless communications and mobile computing,* vol. 8, no. 9, pp. 1227-1232, 2008.

[21] J. Munilla, A. Ortiz and A. Peinado, "Distance bounding protocols with void-challenges for RFID," in *Printed handout at the Workshop on RFID Security–RFIDSec*, 2006.

[22] S. Brands and D. Chaum, "Distance-bounding protocols," in *Advances in Cryptology—EUROCRYPT’93*, 1994, pp. 344-359.

[23] C. H. Kim and G. Avoine, "RFID distance bounding protocol with mixed challenges to prevent relay attacks," in *Cryptology and Network Security*: Springer, 2009, pp. 119-133.

[24] Y. Tu and S. Piramuthu, "RFID distance bounding protocols," in *First International EURASIP Workshop on RFID Technology*, 2007, pp. 67-68.

[25] W. Xin, "Research on the Security and privacy Issues in RFID-Based Supply Chain," Ph.D. dissertation, Beijing: Peking University, 2013.

[26] S. Kang, J. Kim and M. Hong, "Button‐based method for the prevention of near field communication relay attacks," *International Journal of Communication Systems,* 2014, DOI: 10.1002/dac.2751.

[27] P. Urien and S. Piramuthu, "Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks," *Decision Support Systems,* vol. 59, pp. 28-36, 2014.

[28] T. Beth and Y. Desmedt, *Identification tokens—or: Solving the chess grandmaster problem*. Berlin Heidelberg: Springer, 1991.

[29] S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier, and J. Quisquater, "Secure implementation of identification systems," *Journal of Cryptology,* vol. 4, no. 3, pp. 175-183, 1991.

[30] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, 2007, pp. 204-213.

[31] A. Mitrokotsa, C. Dimitrakakis, P. Peris-Lopez, and J. C. Hernandez-Castro, "Reid et al.'s distance bounding protocol and mafia fraud attacks over noisy channels," *IEEE Communications Letters,* vol. 14, no. 2, pp. 121-123, 2010.

[32] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, and B. Martin, "A framework for analyzing RFID distance bounding protocols," *Journal of Computer Security,* vol. 19, no. 2, pp. 289-317, 2011.