A Secured Mutual Authentication Protocol For RFID System

Rajarshi Roy Chowdhury, Md. Abdul Awal Ansary

Abstract: Contactless automatic RFID system is intended to replace existing barcode scheme, since it has the capability of reading huge amount of data from many tags simultaneously in a respective range. Whereas, an RFID system is consist of a database server connected with many readers through wired communication and readers to tags are mostly wireless communication. This wireless connection in between tags and readers are vulnerable by an adversary in many ways. However, there are some common problems in RFID system such as: location tracking, bogus request, indistinguishability, spoofing and forward security. In this paper, we proposed a protocol based on the timestamp and tag's generated random number to overcome such security issues. An additional parameter to use in a tag (random number) will increase some security strength compared to the previous scheme; even though slightly raise processing power in the tag. The anticipated protocol is the extended version of the existing protocol proposed by Cho C., H., Do, K.,H., Kim, J.,W., and Jun, M.,S. in Dec 2009.

Index Terms: RFID, Mutual Authentication, Model, Security, Wireless communication, Tag and Timestamp.

1 Introduction

Radio frequency identification (RFID) is a generic term that used contactless automatic identification system to transmit the identity of an object, animal and so on, wirelessly using radio waves. The RFID tags are consists of small and low-cost microchips and antennas. This is a smart automatic identification technology and day-by-day the usages of RFID systems are booming in public places. The system has been implemented in different ways by different companies; but the global standard of this technology still being under process. RFID tags are easy to conceal or incorporate in a very small item. For example, in 2009, RFID micro-transponders are glued to live ants in order to study their behavior by Bristol University researchers "[1]". However, there are three significant key factors that increased usage of the RFID system, such as: declined cost (equipments and tags, increased performance and a stable international standard around ultra high frequency (UHF) passive RFID, in 2010. Adoptions of these standards were driven by EPCglobal (an organization to achieve worldwide adoption and standardization of Electronic Product Code [EPC] technology), which were responsible for driving global adoption of the barcode in the 1970s and 1980s "[2]". Using RFID technology, it is more efficient way of identifying objects compared to any manual or bar code systems that have been using since 1970s. In addition, passive RFID tags data can be read within close enough to an RFID reader, such as: inside a case, box or other containers. An RFID reader is able to read hundreds or more tags at a time where as a bar code systems can read only one data at a time. This system is using with biometric technologies to provide adequate security.

- *Rajarshi Roy Chowdhury is a Lecturer of CSE department, Sylhet International University (SIU), Sylhet, Bangladesh. E-mail: rajarshiry@gmail.com.*
- *Md. Abdul Awal Ansary is an Assistant Professor of CSE department, Sylhet International University (SIU), Sylhet, Bangladesh. E-mail: awal_sust@yahoo.co.in.*

The RFID system's wide verity of applications are concern about the security and privacy issues have become more and more prominent. Since wireless communication between tags and readers are vulnerable for data breach. Many authentication mechanisms are used and proposed to secure and authenticate each other during data transmission between tag and reader. An intruder can exploits tag's data by using various types of attacks such as: spoofing, reply attack, location tracking and man-in-the-middle attack and many more. In this paper, we analysis a timestamp based mutual authentication protocol for RFID system and pointing out some possible problems such as: location tracking, indistinguishability, forward security, and then proposed a new scheme for mutual authentication. Organization of this paper is as following: in section II and III will give an overview of the RFID system models and characteristics. Security requirement for the RFID systems will explain in section IV. Then, in section V will analyze the selected paper works and identify some security problems. In section VI, proposed a new modified protocol to overcome identified security holes (extended version of the timestamp based mutual authentication protocol for RFID system) and then will do security analysis of the proposed scheme in section VII. Finally in section VIII, draw a conclusion and some future direction of this work.

2 RFID System Model

A typical RFID system consists of three parts: an RFID tag, an RFID reader and a back-end server, as shown in "Fig. 1". A RFID tag consists of a microchip attached to a radio antenna mounted on a substrate. The microchip can store data as much as 2 kilobytes (or more). To retrieve data from a tag (Transponder) using RFID reader, this is a device that has one or more antennas that emit radio waves and receive signals back from a tag. The reader (Interrogator) then passes the information in the digital form to a computer system or a back-end server.

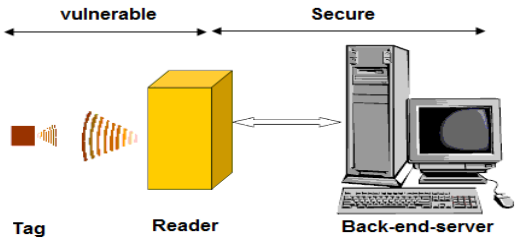

Fig. 1: RFID system model

The RFID tags can be either active or passive. An active tag is prepared with a battery that can be used as a partial or complete source of power for the tag's circuitry and antenna. Some tags enclose with replaceable batteries and some are sealed units. It also contains some transmitter and able to communicates in the long range. They have limited life spans compared to passive tag, even though some of the active tags are build to have up to 10 years life span. However, a passive tag gets their power from the signal sent by an interrogator or reader. It uses this radio waves to convert into power. This means a passive tag is only powered when it is in the beam of the interrogator. It uses backscatter technique to reply to the reader. The passive tag does not involve any transmitter on it, but is a means of "reflecting" the carrier waves and putting a signal into that reflections. Most commonly used RFID tags are passive tags and virtually unlimited life time "[3]".

3 Characteristics And Attack Models Of An RFID System

Each tag has a unique identification number. It seems that EPCglobal of GID-96 is used for a tag ID, which consists of 96 bits. It is the de facto standard, where as used in the supply chain industry "[4]". When a transponder or an RFID tag receives a query from a respective reader, the tag transmits its identification to the reader and then the reader transmits received data to the back-end-server. Since then computer or back-end-sever verifies the tag's authenticity based on their given data. In this system all communication between tags and readers are through radio frequencies, those have some fundamental characteristics:

a. Unique identity of the tag is transmitted to reader without any process.

b. Any reader can get tag's identification by using simple query.

c. Data transmissions are secured between a back-end-server and a reader, where as tag's to reader's communication are not secured.

RFID systems are vulnerable because of these characteristics, and they can cause data leakage. There are some common attack models:

a. ***Privacy problem:*** An RFID tag does not able to differentiate between a legitimate reader and an adversary reader. As a result, an adversary can get information about a product or other information regarding the attached object. An RFID readers or scanners are portable and able to get data from distance (few inches to few yards). Therefore tag's data can be readable without any prior knowledge of the users, which lead to violate user's privacy "[5]".

b. ***Man-in-the-middle attack:*** In which an adversary impersonates a legitimate tag or reader to collect RFID data or metadata during communication (wireless). This is closely related to the replay attack, where as an opponent transmits response message to a reader or a tag, which is obtained from a legitimate reader or a tag by impersonating "[4],[7]".

c. ***Replay attack:*** An adversary can capture data during authentication process in between tags and readers through eavesdropping or traffic analyzing and then transmit back captured messages to tags or readers as legitimate users.

d. ***Brute force attack:*** This type of attacking method is also called a traffic analysis assault. Whereas, an intruder analyze the data traffics between tag and reader and then gets necessary secret information for an authentication protocol or others (such as: to get tag's data, define tag's owner identity and connect to reader). It involves simple methods, for example message eavesdropping during communication or data transfer "[4]".

e. ***Eavesdropping / scanning:*** In an RFID system communication between tags and readers are based on radio frequencies. Therefore the system is vulnerable by adversary. They can get secret information or data through eavesdropping on traffic and able to do various types of attacks "[4]".

f. ***Physical attack:*** Low cost RFID systems architecture has fatal defect, which makes it vulnerable by attackers. There are two types of physical attacks invasive (micro probing, focus ion beam editing) and non-invasive (power/time analysis, radio finger printing). The main goal of these types of attacks are reverse engineering process for crypto algorithm, extract key, physically obtain a tag's data and counterfeit it "[4], [7]".

g. ***Location tracking:*** Using a malicious RFID reader an adversary able to send simple query to tags and from feedback gets the tag's information; and then define the precise tag based on received information analysis. Basically, all tags have unique identity and carry object related information, where it is attached with. As a result, the location of a specific tag exposed, as well as object's identity "[4]".

h. ***Cloning attack:*** Unique identification is the most significant characteristic of an RFID system. Therefore, an adversary able to duplicate or manipulate an RFID tag's data to create an identical RFID tag and which will be able to access or use in an application as a valid tag "[7]".

In this paper assume that in between computer system or back-end server and RFID reader data transmissions are being secured, where as in between RFID readers and passive tags data transitions are not secured. Radio frequencies (wireless) are being used for data communication between them.

4 Security Requirement For The RFID System

For RFID technology sound authentication mechanism in between tags and readers are remain a challenging problem for system implementers and developers. So that, there are some basic security requirement needs to consider throughout the development or accomplishment of RFID authentication mechanism. Generally proper authentication practices able to prevail over privacy and forgery problem in the RFID system. For this study, security requirements are categories into four parts, as follows:

a. ***Indistinguishability:*** To evade real time tracking of a specific tag's location by an adversary using same reader to violate tag owner's privacy. Therefore, it is necessary transmitted tag's information should not be the same.

b. ***Confidentiality:*** During data transmission between tags and readers without any proper authentication mechanism or encryption, an attacker may be able to eavesdropping on data traffic and violate data privacy. For data confidentiality, a reader or a tag is necessary to authenticate each other before transmitted any valuable data, so that only legitimate tag or reader able to read transmitted data.

c. ***Forward security:*** To ensure forward security, a tag's earlier transmitted data should not reveal any information about currently transmitted data. There should not be any relation between current and previous data traffic to avoid serious privacy infringement by an intruder.

d. ***Mutual authentication:*** It is crucial that before any private data transmission in RFID systems they should be authenticated each other with secure manner. The mutual authentication procedures avoid data forgery problems in the system, such reply attack, man-in-the-middle attack.

5 Analysis On The Scheme

There are many authors or researchers have been proposed various security mechanisms for the RFID system based on primitive cryptographic techniques. They used some common mathematical operations to develop their protocols such as: exclusive OR (XOR) operation, hash function, time-stamp and lightweight cryptographic algorithms. In this paper mainly focuses on the timestamp and hash function to provide a secure mutual authentication mechanism during data transmission. In this section will analyze only the problems based on the chosen paper proposed protocol "[8]". Timestamp based RFID mutual authentication protocol shown in "Fig. 2". In this scheme, a tag always generates a random number to response a reader $H(ID \| Rr) \oplus Rr$, based on the legitimate reader's generated random number *Rr*. As a result this protocol is location tracking protected. In addition, the scheme is also secured against reply attack and spoofing. But from the study shown that one way hash function always generates same output for the same input, so if an intruder use a specific reader to generate same number and then send to a tag (step 1) and capture the responded message from the tag (step 4). After may trial and movement of a malicious reader able to track real time location for a specific tag. This method is violating the privacy issue of the tag owner's or data. However, the scheme does not satisfied indistinguishability security requirement as well, because if a malicious reader able to send same number during a request to a tag (step 1), then the response message (step 4) is always same from the tag. The scheme also leaks of confidentiality issue, because time-stamp sends as a plain text from reader to tag (step 2). If malicious reader sends a query after the (step 4) process and the tag replace its time-stamp value *T* and then a legitimate reader reply back on (step 7) to tag, where tag's comparisons will not match (time-stamp values), that means the legitimate reader becomes unauthenticated.

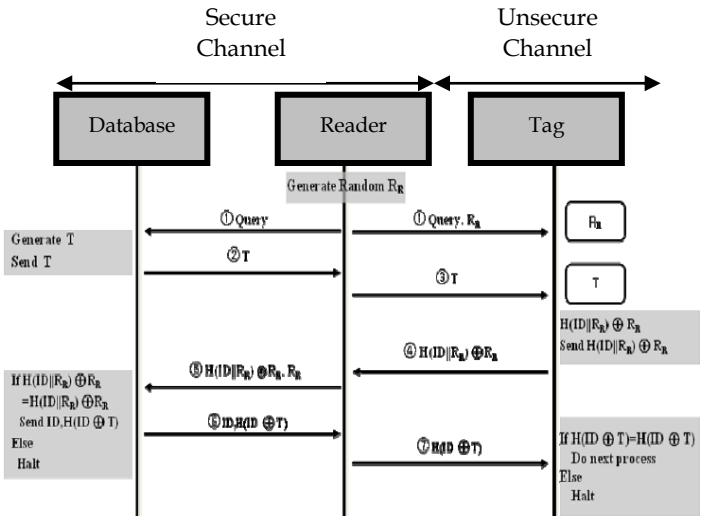

Fig. 2: RFID mutual authentication based on time stamp

6 The Proposed Protocol

This proposed protocol is the extended version of the existing timestamp based mutual authentication protocol "[8]". This diagram illustrates the specify steps, shown in "Fig. 3".

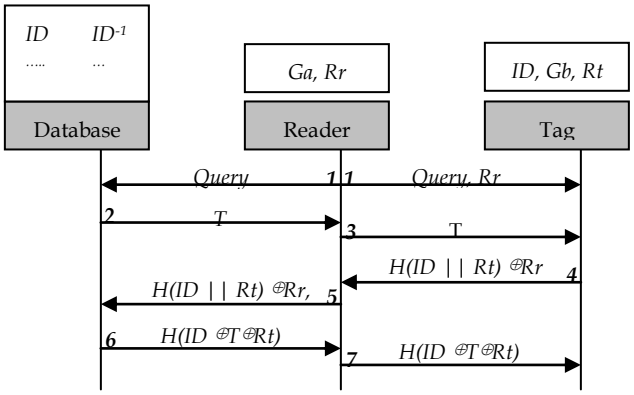

Figure 3: Process of proposed protocol

In this proposed scheme, in between database and reader communication channel is secured and unsecured channel between reader and tag. Additionally, each tag has a random number generator *Gb*. The anticipated protocol implementation details are as follows:

- In the range of communication, the reader first generates (generator *Ga*) a random number *Rr* and send a query to the tag and database at the same time.

[Database] *Query* ← Reader → *Query, Rr* [Tag]

Database: When it gets a query to produce a timestamp *T*.

Tag: To store *Rr* in its subjective storage and generate a random number *Rt* after acquires the query.

- *T* (Timestamp) is send to the reader from the database.

  Database → *T* [Reader]

- The reader sends received *T* to the tag.

  Reader → *T* [Tag]

Tag: After receiving the *T* from the reader, it stores *T* in arbitrary storage for future verification.

- The tag calculates a hash value using its *ID* concatenating with a random number *Rt* and then the result is *XOR* with stored *Rr*. The value $H(ID \| Rt) \oplus Rr$ is send to the reader.

  Tag → $H(ID \| Rt) \oplus Rr$ [Reader]

- The reader sends received message $H(ID \| Rt) \oplus Rr$ and *Rr* to the database.

  Reader → $H(ID \| Rt) \oplus Rr$, *Rr* [Database]

- After received the message from the reader, database generates $H(ID \| Rt) \oplus Rr$ using the value stored in its storage such as: tag *ID* and ID^{-1}. If the values are equal then **the tag is authenticated** and calculate $H(ID \oplus T \oplus Rt)$, else the system would not response anything to the reader (stop working).

  Database → $H(ID \oplus T \oplus Rt)$ [Reader]

- If the reader gets response from the database $H(ID \oplus T \oplus Rt)$ then send the received message to the tag. After that the tag will generate $H(ID \oplus T \oplus Rt)$ from its storage value and compare with the received message. If the comparison is equivalent then **the reader is authenticated** and continues to do the process else the tag stop working.

7 Security Analysis Of The Proposed Protocol

The low-cost RFID tags have limited hardware resources to implement complex cryptographic function. Therefore, tags have many limitations for operations, but they are able to perform some primitive operations very fast and efficiently, such as: simple hashing, *XOR* ($\oplus$), random number generation and concatenation ($\|$) operations. However in contrast, an RFID reader and back-end server are capable of doing more complex operation in terms of hardware resources. The proposed protocol consists of seven steps and it performs mutual authentication securely. The scheme is secure enough to prevent location tracking, reply attack, spoofing, indistinguishability and meaningless request. The overall performance is good, because the scheme uses hardware primitive operations. Table 1 and 2 shows respectively the assessment between existing and proposed method in terms of functions and securities.

Table 1
Functional Comparison Between Existing And Proposed Protocol

Note: 1 means number of function/operation.

Protocol	Entity	Operation count				
		Hash Function	Random Number Generator	$\oplus$	$\|\|$	Time stamp
Existing protocol	Tag	1		1	1	
	Reader		1			
	Database	1		1	1	1
Proposed protocol	Tag	1	1	1	1	
	Reader		1			
	Database	1		1	1	1

Table 2
Security Strength Comparison Between Existing And Proposed Protocol

Note: 0 means provide security and x means do not provide security.

Types of Attacks	Protocol	
	Existing protocol	Proposed protocol
Spoofing	0	0
Replay	0	0
Location tracking	?	0
Indistinguishability	x	0
Meaningless request	x	0

From the Table 1 it is clear that the proposed scheme added a new operation "**Random Number Generator**" to improve the level of security. And in the Table 2 shows that, the proposed method secure against location tracking, indistinguishability and meaningless request attacks. Therefore the new proposed system more secure against existing scheme.

Location Tracking: In the proposed protocol, a reader always gets different response from the tag in step 4 $(H(ID \| Rt) \oplus Rr)$ either the reader is legitimate or malicious, because tag generates a random number in every session *Rt*. As a result it is not possible to track the current tag location of a specific tag.

Indistinguishability and meaningless request: The proposed method uses *ID* (tag's unique *ID*) and *Rt* (tag's randomly generated number) to generate a hash value in every session, so it is impossible to use response message to predict required data. The scheme is also secure against meaningless request, therefore the proposed protocol provide complete indistinguishability.

8 Conclusion

The implementation of RFID technology makes object identification and tracking more conveniently in terms of management, since the RFID system is contactless, small size and low-cost. However, the system is suffered from many vulnerable attacks by malicious users to capture data or

manipulation of data during wireless transmission over unsecure communication channel. In order to avoid some issues or problems need to satisfy some of the fundamental security needs. Therefore, we proposed a mutual authentication protocol based on the timestamp for RFID system. The scheme provides two levels of authentication and secure against location tracking, spoofing attacks, indistinguishability and reply attacks. It is not possible to provide complete security, where hardware resources are very limited. For further works, to improve the level of confidentiality.

REFERENCES

[1] Ants' home search habit uncovered, [Link: http://news.bbc.co.uk/2/hi/uk_news/england/bristol/somerset/8011998.stm].

[2] Miles, Stephen Bell. RFID Technology and Applications. London: Cambridge University Press. pp. 6–8, 2011.

[3] High Tech Aid. [Link: http://www.hightechaid.com/tech/rfid/rfid_technology.htm].

[4] J.S. Cho, S.S. Yeo, S.K. Kim, Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value, Computer Communications, pp.391-397, March 2010.

[5] Technovelgy.com - where science meets fiction, [Link: http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=20].

[6] Dimitriou, T., A Lightweight RFID Protocol to protect against Traceability and Cloning attacks, Security and Privacy for Emerging Areas in Communications Networks - SecureComm 05, pp. 59 - 66, September 2005.

[7] NEOCATENA NETWORKS INC. (Next genaration RFID Security) [Link: http://neocatena.com/technology/risks/].

[8] Cho C.,H., Do, K.,H., Kim, J.,W., and Jun, M.,S., Design of RFID Mutual Authentication Protocol using Time Stamp, 4th International conference on computer sciences and convergence information technology, December 2009.