ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

A SIP Based Authentication Scheme for RFID Systems

Shruti S.Utpat[#], Parikshit N.Mahalle.[*]

Abstract: **In today's world of technology the biggest challenge for RFID technology is to provide benefits without threatening the privacy of consumers and providing secure authentication for RFID tags. Previously many solutions had suggested but there were many ways to break them. An approach of TRAP family of protocols by Tsudik seems to provide secure authentication but it is vulnerable to Denial-Of-Service (DOS) and replay attacks. This paper presents a novel method for secure authentication of RFID tags using cryptographic approach. The protocol is an improved version of YA-TRAP and YA-TRAP* family of authentication protocols. The proposed protocol is SIP based implementation aims to authentication of RFID tags.SIP provides benefit of running a particular session for one tag. The protocol can be applicable for tracking applications. The main contribution is to resist attacks on RFID systems.**

Index Terms-: **Secure authentication protocol, tag level counter, TRAP family of protocols.**

I.INTRODUCTION

Radio Frequency Identification Technology (RFID) has become ubiquitous in our everyday life; it is a recommended technology as it has several features like contact-free communication. The RFID technology now a day's replaced barcodes by reduction in cost and efforts for product identification. The use of RFID in tracking and access applications first appeared during the 1980's.The RFID system is composed of three parts: RFID tags, reader and a server(backend database).Tag is called as transponder, as it responds to the reader's challenge. Reader perform role of reading the data coming out of a tag, and sends tag's message to server. Server will reveal the received data and authenticate the tag. However, the major flaw in RFID system is, which inhibits the authentication, is security and privacy issues in this technology [1].

To provide privacy and security researchers provide cryptographic approach for authentication of tags. In this paper, we present a cryptographic RFID authentication protocol for tag authentication.

As compared to other approaches here, we have employed cipher instead of a hash function. Instead of timestamp value, we have employed counter at tag level. In addition, our protocol improves on previous schemes in number of computations at server and tag level is deterministic.

II.BACKGROUND AND MOTIVATION

In past few years, numerous families of authentication protocols have been evolved, each of these having an intrinsic idea. Most secure authentication protocols for RFID uses the cryptographic approach. One of the first cryptographic privacy enhancing technology for RFID is the hash-lock by Weis.S. [2].The idea behind the proposed scheme includes one assumption that tags cannot be trusted to store long-term data; the author has suggested the mechanism to lock the tag without storing the access key, but only stores hash of the key on the tag. Then the Henrici.D [3] have later extended randomized version of the original hash lock protocol for increasing privacy and scalability. Later Avoine.G. [4] Proposed hash-based RFID protocol, which provides modified identifiers results in improving privacy and that, can be applicable for authentication. In that, mechanism authors concentrates on issues regarding scalability of privacy enhancing scheme, which introduces a specific time-memory trade-off.

Later Hwang Y.J **[**5**]** proposed a method for authentication tags in low-cost RFID systems .All the above protocols are based on synchronized secrets residing on tag and backend database and they require one-way hash function from the tag. After this Juels.A. [6] Presented an approach to increase, tracing and forgery resistance of RFID banknotes uses digital signatures for authentication. It uses re-encryption, which resists static identifiers and optical data on the banknote to attach RFID tag to the paper. Authentication has been done by verifying that the data on tag is signed by using valid public key. In order to resist to cloning attack authors have suggested including some distinctive characteristics of the physical media into the signature and then verifying the validity. Later this scheme enhanced by Zhang X [7], which then addressed some integrity issues. Later the protocol on which proposed scheme is prominently based was YA-TRAP the protocol provides mainly tracking resistance with tag authentication through sequentially increasing timestamps on the tag. The protocol needs in built PRNG (Pseudo-random number generator) in the tag, but the original protocol is vulnerable to DOS attack because of timestamp resynchronization between tag and the server. The computation of back results of previously computed hash table will reduce the server search load. However, later Chatmon.C [8] proposed a protocol based on YA-TRAP would increase server load tremendously. The approach after this proposed by M.Rahman. [9] Which is named as YA-TRAP* which uses XOR function to combine several tag responses which again reduces the reader to server communication cost. They have used authentication tokens in protocol. Again, this idea was vulnerable to higher cost while sending tag responses to the server.

As these families of authentication, protocol was having the problem of timestamp value update at the tag level. The problem was, though token can validate timestamp but a tag cannot assure that message is coming from trusted reader. To overcome with this we have introduced a tag level counter in our protocol, which is incremented initially as reader challenges the tag and tag responds to reader. The incremented counter will then send to the server in an encrypted manner. Here we have also employed cipher instead of a hash function to provide more security. When server will receive the message, it will reveal the new

counter value and store it. The malicious parties may enter in system by querying tag and incrementing tag counter but as we are storing each tag value from previous authentication round we can compare previous counter value of the tag with the new counter value, if the counter has incremented then the tag can be believed to be authentic.

III.PROPOSED PROTOCOL

The proposed protocol introduces key classes, for reducing computational load at tag side and server side, the database at the server side associates key class, tag related data like counter value as shown in Table 1. A key class number (Kn) identifies the key class, all tags present in that particular key class uses same pair of keys (Key_1, Key_2) to encrypt their messages. The tag's binary id is divided into two parts, as upper ID and lower ID. The upperID of the tag will be unique within a key class. Additionally the server database relates tag's ID with the authentication counter T_{cold} at the tag level. As tag sends its key class number to the server, the server can immediately fetches the exact keys and decrypt the tag's messages. As server uses key classes there are no possibilities of exhaustive key search at server level, in result to this the number of computations at server side are deterministic. Here we have made one assumption, that a tag is equipped with a *pseudo random number generator* (PRNG) and it stores its authentication counter, two encryption keys and a authentication counter in it.Also,tag can compute a cipher. The initial counter of the tag will be zero; the tags authentication counter will be half of the bit-width of the tag's ID.

The server database will be as,

TABLE I: SERVER DATABASE-KEY CLASSES.

Key class no.(K_n)	Tag ID		Tag counter	Key Pair	
	ID_1	ID_2		Key_1	Key_2
1	0	1	0	3	6
1	1	3	0	6	5
.	.	.	.	.	.
.	.	.	.	.	.
2	2	0	0	4	3

Colored part shows first part of tag ID should not repeat within same key class.

The protocol will be initiated by the reader's challenge for the tag, as shown in fig.1 the reader challenges tag by sending a random number R_r to the tag in message m_1, this random number is valid for each tag participating in that particular authentication round, for each new round the reader will compute new random number. As tag receives the reader's challenge, it will compute its random number R_t and increments its counter T_c by one. Then it covers its original ID and its authentication counter by enciphering both of them using key pair associated with its key class,

The equation will be as,

$$h_1 = ((R_r \| R_t) \oplus ID, Key_1) \quad (1)$$

As Equation 1shows,the tag's ID is covered by its random number, as we have divided tag's ID in two parts, in equation1 the reader's random number covers upper part of the tag's ID and tag's random number covers lower part of tag's ID, this result is then encrypted to h_1 using Key_1. The second key from key class is used for the second operation of calculating equation 2,

$$h_2 = h((R_r \| 0) \oplus (R_t \| R_t) \oplus ID \oplus T_c, Key_2) \quad (2)$$

The equation covers the authentication counter by using tag's and reader's random number, after completing all computations tag will send all encrypted data, its key class and its random number to the reader through message m_2.

As reader receives message from tag, it concatenates its random number and all tag's messages in one message and then forwards it to the server.
To authenticate a tag, server first fetches the keys from key class of that tag, then it will decrypts h_1 and h_2.The server will first reveal only the upper part of the tag ID. As the upper part of the tag ID is unique within particular key class, the server can easily find out lower part of the tag ID, and can check for stored value of tag counter i.e.$T_{cold.}$ Here server is not required to reveal the tag's random number from equation h_1, as in message m_2 we are sending tag's random number also in concatenation with key class, equation h_1 and equation $h_2$and then it will be able to reveal authentication counter T_c of tag for recent authentication round. To authenticate that tag server will check if, $T_c > T_{cold}$ then the tag is authenticated, to prevent cloning attack. The authentication condition will be, as the tag is authenticate only when the current counter value is incremented by one in comparison with the old counter value.

After authentication, the new counter value will be updated to the database. In addition, server will send authentication message m_3 back to reader.

The protocol has also implemented Session Initiation Protocol (SIP), so if one session of authentication is going on no another tag can interrupt the session, the reader will restrict the reading of next tag in between first session. After completion of authentication of first tag then only the next tag will be authenticated. This will help to track the attacker's tag.

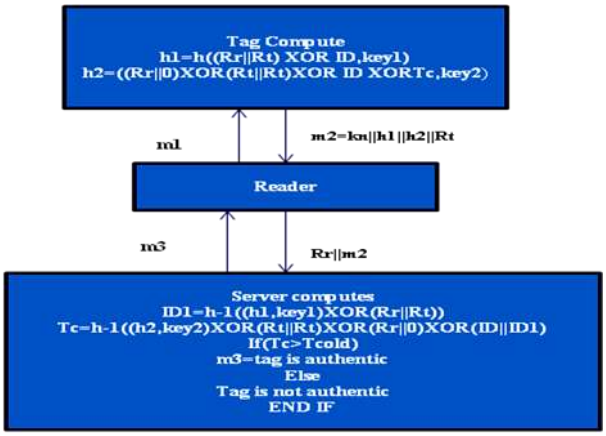

Figure 1 :Message flow in proposed protocol

IV. EXPERIMENTAL SETUP AND IMPLEMENTATION

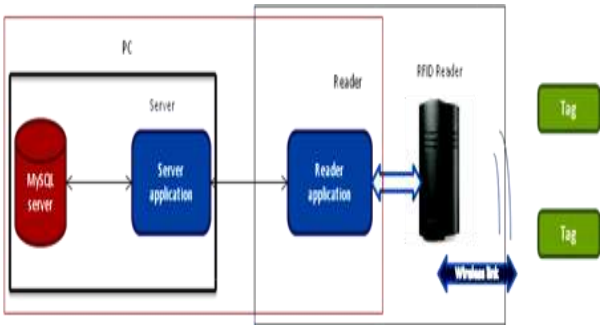

Fig.2 Experimental Setup

We have presented the cryptographic implementation of this authentication protocol on passive RFID tags. As shown in fig.2 the protocol is implemented in a typical RFID environment. The reader and server software are implemented on C#.Net platform. The difference between them is in the entity they interface, i.e. for server it is MYSQL database and for reader software, it is the RFID reader. Though it is a cryptographic protocol instead of employing hash function for computation, we have employed cipher. The Ceaser Cipher is the adaptable cipher for this scheme, as it provides too many combinations for keys required. In addition, it is difficult to break cipher for attackers. The system consists of passive (computation capable) tags, RFID reader and a computer, which runs the reader, and server application software. The server application provides interface to a MySQL database, which stores all the information of tag side and server side. The implementation details of these RFID entities are as follows:
We have employed passive and computation capable 64 bits tags.
The reader is a combination of RFID reader and software that runs on PC. The reader software itself controls the protocol flow.
The server is composed of MySQL database that stores all the information about data required for computation on server side and tag side, and interface software that establishes connection with reader software.

Implementation:
RFID tag is read by reader and tag increments its counter by one. Here tag's computation part will be performed by tag's application software called as tag simulator, which will display all the computations performed by tag. After completing encryption of all data by using cipher, the data will be sent to server through reader which is nothing but reader application, then server will reveal all the encrypted data on application software and gives authentication of tag by comparing previous value of tag counter which is stored in MySQL database with the new value. After this, it will update the database with new values. Fig 3 and Fig.4.showsresults.

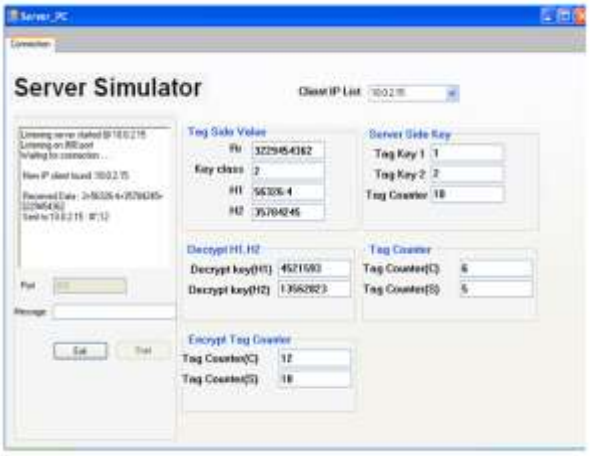

Fig 3: Server side values after tag authentication.

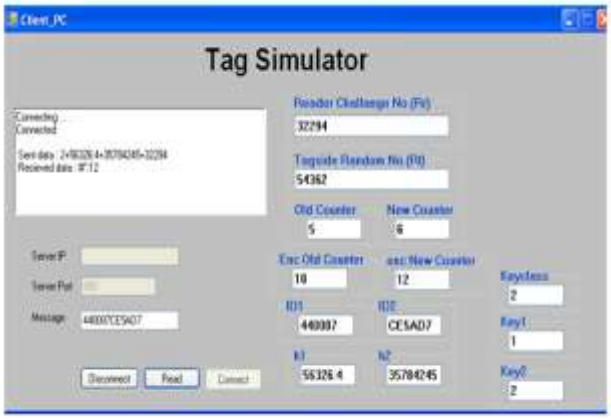

Fig 4: Tag side values after authentication.

As, during each authentication round of protocol the required data will be read and write from the tag. As the tags used are passive but are computation capable and can be read from possible range of distance,Fig.5 and Fig.6 shows the graphical analysis of time required to read/write data to/from the tag at each possible distance(in cm's).

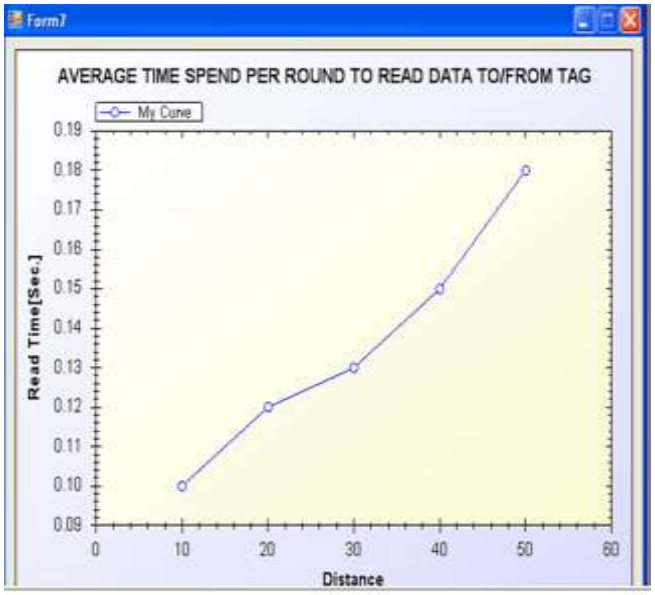

Fig 5:Average time required to read data to/from tag.

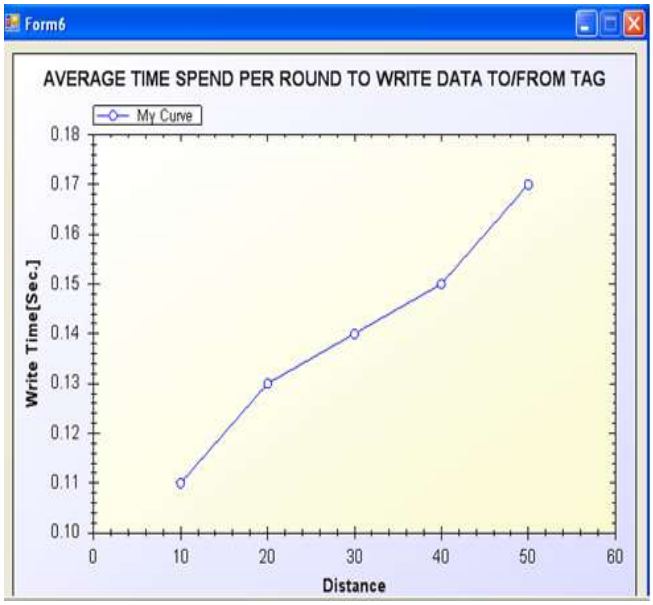

Fig 6.Average time required to write data to/from tag.

V.SECURITY ANALYSIS

The proposed protocol offers security and attack resistance.The protocol resist DOS attack,by querying a tag malicious parties can increment authentication counter T_{cold} ,but it will not affect as the authenticity of tag is confirmed when counter is incremented.so there is no possibillity of DOS attack by malicious parties,and to reduce some possibillity of such attack we are using tag's authentication counter >=32bits.As protocol is checking for only one incrementation of value of authentication counter it is resistant against replay attack.

VI.CONCLUSIONS

This paper is presenting a cryptographic authentication protocol for RFID systems.The protocol is advancement over TRAP family of protocols.The protocol is using passive but computation capable tags so the protocol can resists attacks like Denial-Of-Service attack,cloning attack.The computation time is also reduced as the protocol is using Key Classes for storage.The implementation verifies superior nature of protocol.

VII.REFERENCES

[1] SocietyA. Juels, "RFID security and privacy: a research survey," IEEE Journal Selected Areas in Communications, vol. 24, no. 2, pp. 381–94, Feb. 2006.

[2] Weis, S., Sarma, S., Rivest, R., and Engels, D. (2003). "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems". In D. Hutter, G. Müller, W. Stephan, and M. Ullmann, editors, International Conference on Security in Pervasive Computing - SPC 2003 Conference on Computational Science and its Applications - ICCSA 2005, Proceedings.

[3] Henrici, D. and Müller, P. (2004). "Hash-based enhancement of location privacy for radiofrequency identification devices using varying identifiers". , International Workshop on Pervasive Computing and Communication Security – Per-Sec 2004, pages 149–153, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer.

[4] Avoine, G. and Oechslin, P. (2005). "A scalable and provably secure hash based RFID protocol". In International Workshop on Pervasive Computing and Communication Security – PerSec 2005, pages 110–114, Kauai Island, Hawaii, USA, March 2005. IEEE, IEEE Computer Society Press.

[5] Lee, S.M., Hwang, Y.J., Lee, D.H., and Lim, J.I. (2005). "Efficient authentication for lowcost RFID systems". In Osvaldo Gervasi, Marina Gavrilova, Vipin Kumar, Antonio Lagana`a Heow Pueh Lee, Youngsong Mun, David Taniar, and Chih Jeng Kenneth Tan, editors, International.

[6]Juels, A. and Pappu R. (2003). Squealing Euros: "Privacy Protection in RFID-Enabled Banknotes". *In Rebecca N. Wright, editor, Financial Cryptography -- FC'03, volume 2742 of LNCS, pages 103--121, Le Gosier, Guadeloupe, French West Indies, January 2003. IFCA, Springer-Verlag.*

[7] Zhang, X. and King, B. (2005). "Integrity Improvements to an RFID Privacy Protection Protocol for Anti-counterfeiting". In Jianying Zhou, Javier Lopez, Robert Deng, and Feng Bao, editors, Information Security Conference – ISC 2005, volume 3650 of Lecture Notes in Computer Science, pages 74–481, Singapore, September 2005. Springer-Verlag.

[8] Chatmon, C., Le, T.v., and Burmester, M. (2006). "Secure anonymous RFID authentication protocols". Technical Report TR-060112, Florida State University, Department of Computer Science, Tallahassee, Florida, USA, 2006.

[9] M. Rahman, M. Soshi, and A. Miyaji, "A secure RFID authentication protocol with low communication cost," Mar. 2009, pp. 559–564.

AUTHORS

First Author – Shruti S.Utpat, M.E.(Computer Networks-pursuing), Smt.Kashibai Navale College of Engineering.

Second Author – Parikshit. N.Mahalle, M.E.(computer Engineering), PhD(Pursuing),Smt.Kashibai Navale College of Engineering.