A Secure Authentication Scheme for Ubiquitous Computing

Shruti S.Utpat
Master of Computer Engineering (Computer Networks)
Smt.Kashibai Navale College of Engineering.
Pune, India.

Parikshit N.Mahalle
Department of Computer Engineering
Smt.Kashibai Navale College of Engineering.
Pune, India.

ABSTRACT
Ubiquitous Computing is the method of enhancing computer use by making many computers available throughout the physical environment, but making them efficiently invisible to the user. The ubiquitous networking capabilities support various classes of applications/services which require "Any Services, Any Time, Any Where and Any Devices" operation. As in ubiquitous computing identity of object and its authentication to the system plays a very vital role. So, it is important to have a technique through which we can read the object. After reading there will be the next role of identification and authentication of the object. As in ubiquitous computing identity of object and its authentication to the system plays a very vital role. 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 proposed protocol is SIP based implementation aims to authentication of RFID tags.SIP provides benefit of running a particular session for one tag. The main contribution is to resist attacks on RFID systems.

General Terms
Computer networks, Security.

Keywords
Secure authentication protocol, tag level counter, TRAP family of protocols.

1. 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 is replacing barcodes by reduction in cost and efforts. 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. 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.

2. BACKGROUND AND MOTIVATION
Over the past years, various protocol families have evolved, each of these having an intrinsic idea. Most secure authentication protocols for RFID uses the cryptographic approach.

One of the first cryptographic schemes was hash lock proposed by Wei's et.al.[2] The idea proposed was to lock the tags and that too without storing access key on the tag but only storing hash of the access key on the tag. The scheme resists cloning attacks so it is more suitable for protecting privacy. Later Avoine et.al proposed another hash based protocol [3] by introducing a specific time memory trade off in a scheme by Ohkubo et.al named as "cryptographic approach to privacy friendly tags." Later Hwang Y.J [4] 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 et.al [5] presented an authentication approach of RFID authentication by using digital signatures it uses re-encryption. After this Juels [6] proposed minimalist cryptographic approach for authentication but the protocol was aimed to mutual authentication so the communication cost was relatively high as compared to previous ones. After this, Juels has [7] proposed low cost authentication protocol. Later the protocol on which proposed scheme is prominently based was YA-TRAP [8] (Yet another Trivial Authentication Protocol) 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 end results of previously computed hash table will reduce the server search load. But later Chatmon.C [9] proposed a protocol based on YA-TRAP will increase server load tremendously.

The approach after this proposed by M.Rahman [10] 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. But again this idea was vulnerable to higher cost while sending tag responses to the server. Kirk H.M. [11] proposed cryptographic protocol for apparel products. Y. Zhang [12] presented an informative on RFID and sensor networks architectures.

2. PROPOSED SCHEME

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 1: 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,

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

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,

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

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 m2.

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 decrypt h1 and h2.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 authenticated 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.

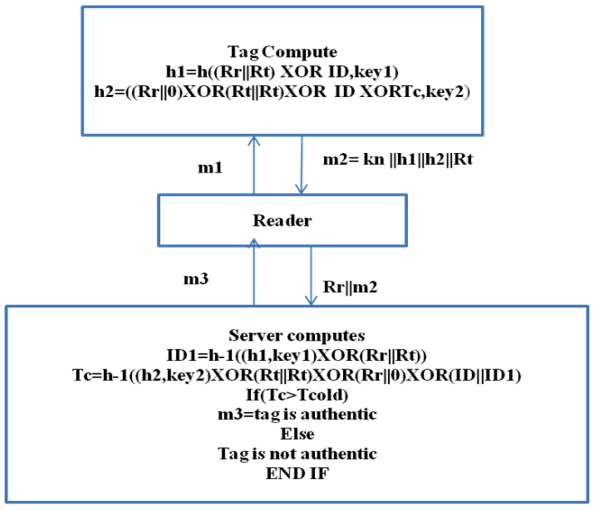

Fig.1:Message flow in Proposed Scheme

3. IMPLEMENTATION

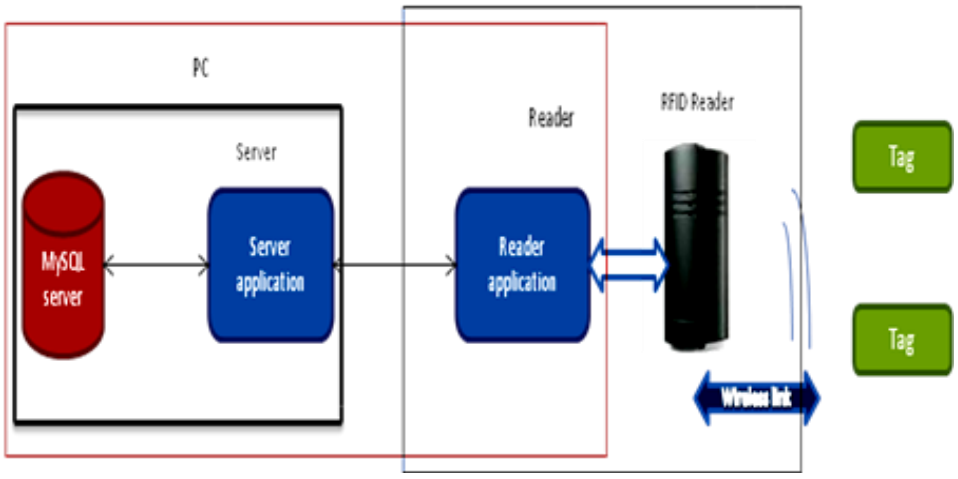

Fig.2: Experimental Setup

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 Ms-SQL 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 Caesar 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 Ms-SQL 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 Ms-SQL 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.

4.1 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 Ms-SQL database with the new value. After this, it will update the database with new values. Fig 3 and Fig.4. shows results.

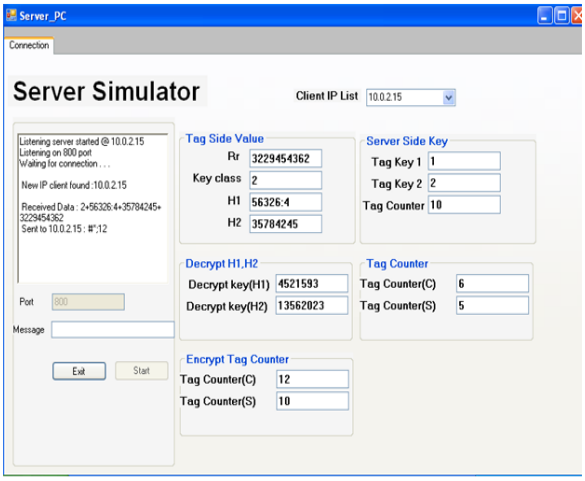

Fig 3: Server side values after tag authentication.

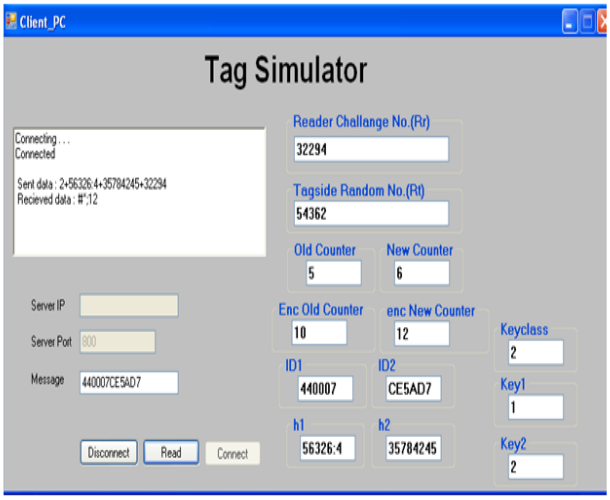

Fig 4: Tag side values after authentication.

5. RESULTS AND DISCUSSIONS

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. The Table 2 shows average time to read or write data to/from tag keeping it at a variable distances.

Table 2: Average times spend to read/write to /from the tag.

Distance	Read(s)	Write(s)
10cm	0.10	0.64
20cm	0.12	0.65
30cm	0.13	0.66
40cm	0.14	0.68

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).

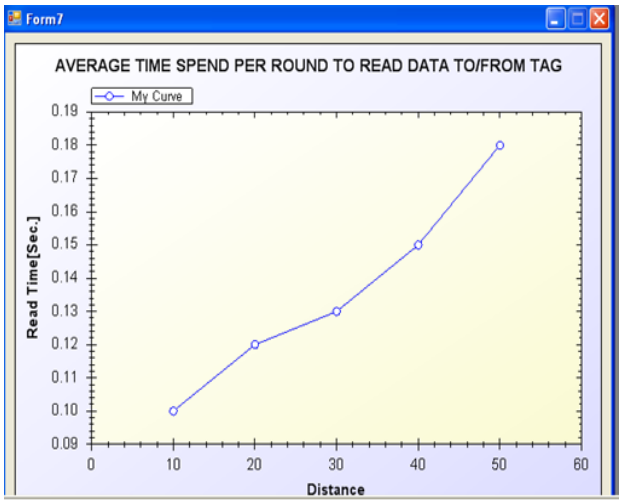

Fig 5:Average time required to read data to/from tag.

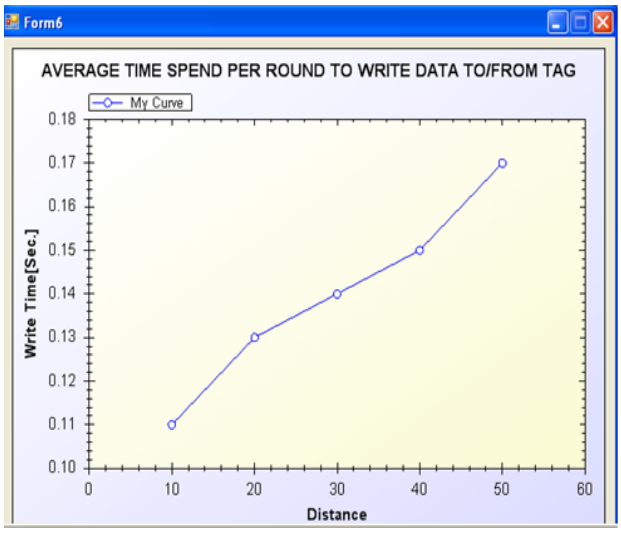

Fig 6.Average time required to write data to/from tag.

The key classes used on server side helps to reduce the seaching time for a tag entry in database. The reading shows as the number of registered tags to the database increases the time required to search will be efficient.

Table 3:Computational time at server side

No. of tags	Time required to search tag in seconds	
	Proposed Scheme	Previous Scheme
5	0.30	0.66
10	0.32	0.72
20	0.40	0.85
30	0.46	1.10

As, the table shows the values of tag search on server side, in previous schemes no key classes used so the searching time was high as compared to proposed scheme. Depending on key class number the server [1] directly searches into exact field so the search time is reduced.

6. 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.

7. CONCLUSIONS

In this project secure authentication scheme for RFID system is proposed. The RFID is an immensely growing technology in today's world. , but along with its benefits the possible vulnerabilities of system should also be considered. The presented scheme is a novel method which implements one way authentication. The scheme consumes less time and implements session initiation technique which can used for attacker tracking.

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

8. 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] 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.

[4] 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.

[5] 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.

[6] Juels, A. (2004). "Minimalist cryptography for low-cost RFID tag". In Conference on Security in Communication Networks -- SCN'04, LNCS, Amalfi, Italia, September 2004. Springer- Verlag.

[7] Juels, A. (2005). "Strengthening EPC Tags against Cloning". In M. Jakobsson and R. Poovendran, eds., ACM Workshop on Wireless Security (WiSe), pp.67-76. 2005.

[8] G. Tsudik, "YA-TRAP: Yet another trivial RFID authentication protocol," in Proc 4th IEEE Int Conf Pervasive Computing and Communications Workshops. Washington, DC, 2006, pp. 640–643.

[9] 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.

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

[11] Kirk H.M. Wong, Patrick C.L. Hui, Allan C.K. Chan "Cryptography and authentication on RFID passive tags for apparel products" in Computers Industry 57 (2006) 342–349.

[12] Y. Zhang, L. Yang, and J. Chen, Eds., "RFID and Sensor Networks: Architectures, Protocols, Security and Integrations", New York: CRC Press, 2010