A Novel RFID Authentication Protocol with Ownership Transfer

Dong Sun, Dan Liu
Department of Computer Science & Technology
Henan Mechanical and Electrical Engineering College
Xinxiang, Henan 453003. China
dongdong@163.com

JDIM
Journal of Digital Information Management

ABSTRACT*: During recent years,RFID technology has a wide applications in many fields.Since singnal transmit by the radio frequency, it raises many security and privacy concerns. Ownership transfer of RFID tags is another requriement for RFID systems. During the life of tag, it may pass from manufacutrer to commercial agent, the ownership of tag need change correspondingly.Taking into account the natural security flaws in RFID systems, it is a challenge to design an authentication protocol with ownership transfer. In this paper, we propose an RFID security method that achieves all requirements based on xor and Public Key Infrastructure (PKI). In addition, we prove it with BAN logic.*

Categories and Subject Descriptors:
D.4.6 [Security and Protection]: Authentication; **G.1 [Numerical Analysis]:** Numerical Algorithms

General Terms:
RFID, Public Key Infrastructure, Radio Frequency

Keywords: RFID, Authentication, BAN, Security and Privacy, Radio Frequency, Public Key Infrastructure

Received: 2 July 2013, Revised 27 August 2013, Accepted 31 August 2013

1. Introduction

Radio Frequency Identification is one of the fastest developing techniques in recent years. This technology is widely used in many fields, such as retail trade,libraries, car tracking, product identification and passport.RFID will be a substitution for bar code in the near future. This technology facilitate our lives. It is expected to play an important role in the future.

RFID systems consist of three components including radio frequency tags, readers, and a back-end database server. An RFID tag is a micromini device, which include a small microchip. It has a low capability of computing. According its usage, it can be classified into two categories: (1) passive tags: it have no inside power supply. Reader will provide outside power when reader performance a query request. Tags can broadcasting singnal with no physical contact. (2) active tags: it have inside pover supply such as batteries. Reader is a device that can read the information from tag .Then forward the received information to the back-end database server to identify whether it is authenticated. After being authenticated, reader can obtain the information of tag, such as ID, owner etc. Database server is a database which store the information of tag. In this paper, not only it can authenticate tags, but also it is a trust third party in ownership transfer.

Our major contribution in this paper is to present a security and privacy method for RFID group ownership transfer based on public key infrastructure and *xor*. Proposed method not only security but also efficient.

This paper is organized as follows. Section II describes security problems of RFID and related work.In section III, a new mutual authentication method is described. Its security will be proved by Ban logic in section IV. In section V, we draw a conclusion.

2. Security Problems and Related Work

Tag, reader and database server make up RFID system. Tag communicate with reader by radio frequency. It is a wireless channel, so the system is apt to suffer from the attacks of interception and eavesdropping. Reader communicate with database server by network. It maybe local network or Internet. Also it is not safe. The main attacks the system may suffer just like follows:

2.1 Impersonation

Attacker forge a tag or reader as an authenticated one to steal the imformation in database server.

2.2 Eavesdropping

It is easy for eavesdroppers to get the singnal from the open wireless circumstance, that lead to the business

information to be leaked.

2.3 Replay attack
After the information of tag leak out, attacker transmit the information he get and spoofs as legitimate tag.

2.4 Dos attack
Attacker transmit some messages to interrupt the communication among tag, reader and database server.

2.5 Asynchronization
The difference between the key in tags and the one in databse means the authenticated tag can not be recognized. This may happen in group ownership transfer.

2.6 Windowing problem
This means dual ownership for the tag during time gap. Both old owner and new owner possess permission to control the tag.

Previous papers have do some research in RFID security, however, many protocol have some risks in security. Several previous papers want to achieve mutural authentication; unfortunately, except for Chien and Chen's protocol [1], they can not completely achieve all the security requirements as described . nevertheless, Chien and Chen's protocol can be secure only assuming that the channel between the reader and the database is secure [2]. Osaka [3] and Cao [4] proposed a protocol to achieve group ownership transfer, but it maybe leak out the owner's privacy. Tripathy and Nandi [5] adopt a dynamic ID to avoid replay attack but it may suffer Dos attack. We conclude three methods form previous papers to diminish security risks the RFID system confront.

(1) Hash. Many protocol adopt hash function to avoid simply transmission. Hash function can not reverse, so attacker can not get the true meaning even if he intercept some message.

(2) Random. Random numbers are added in many protocol to defense replay attack. even if attacker intercept some message in an open channel, he can not access database server or tag because random numbers have changed.

(3) TTP (Trust Third Party) In an ordinary way, database server play a role of trust third party in the process of mutual authentication between reader and tag. But this strategy may result in asynchronous.

3. Proposed Method

In this section, we propose an RFID security method that achieves all requirements based on a xor and public key Infrastructure.

The following notations are used throughout this paper:

Ek ( ) Encryption function (under key k); It maybe xor, symmetrical encryption or asymmetric encryption, which depends the capability of compution about entity.

D( ) Decryption function;

K & $K1$ The key for encryption; Different group owner have different key, so it can identify the owner of tag. In this paper, $K1$ represent a new owner .

ID The unique identifier of tag;

Rt The random number generate by tag;

Rr The random number generate by reader;

Rs The random number generate by database server;

$\oplus$ XOR operation;

Info (ID) The specific imformation of tag which has this ID.

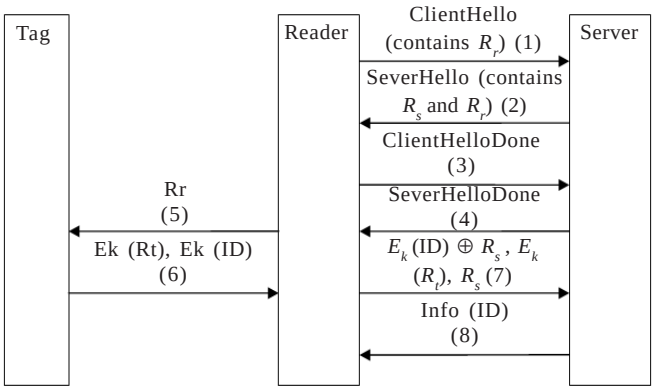

Figure 1. Authentication Process

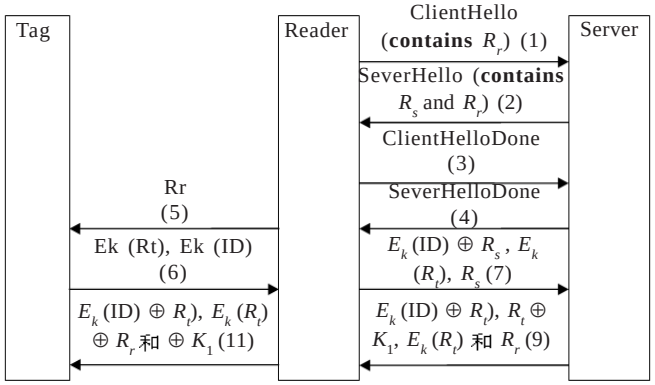

Figure 2 . Ownership Transfer Process

3.1 Protocol Description
Taking into account the power of compution about reader and database server, we assume PKI infrastructure has implemented between reader and server. It means that both reader and server have the public key of each other. The process of protocol depict as follows:

A section of establish a secure communication channel

(1) Reader generate a random number Rr, and transmit a ClientHello (contains Rr) which is encrypted under the public key of server to database server.

(2) Server generate a random number Rs when it receive the random number Rr from reader. ServerHello (contains Rr and Rs) is encrypted under the public key of reader. server transmit ServerHello to reader.

(3) Reader check whether the random number received

from server equal to Rr it stored. If it is equal, store the random number Rs and transmit ClientHelloDone to server. Else it means the message is illegal, so dispose this message and go to step 1.

(4) Server transmit ServerHelloDone to reader when it receive Client Hello Done form reader. It means a secure communications channel has been established.

A section of mutual authentication

(5) Reader transmit a request (contains Rr) to tag .

(6) Tag store Rr and generate a random number Rt. Tag transmit $Ek\,(Rt)$, $Ek\,(ID)$ to reader.

(7) Reader encrypt $Ek\,(ID) \oplus Rs$, $Ek\,(Rt)$, Rs under public key of server and transmit them to server.

(8) Server check whether the random number received from reader equal to Rs it stored. If it is not equal, the protocol is terminated. else server get $Ek\,(ID)$ by compute $Ek\,(ID) \oplus Rs \oplus Rs$. The real ID is got by compute $D\,k\,(Ek$ (ID)). Server search ID in the databse, if it is found, the authentication process is success. Server transmit info (ID) which is encrypted under the public key of reader to reader. If it is failure to find ID, using the key of successful authentication of last time to decrypt $Ek\,(ID)$. if ID is found, the authentication process is success. Server transmit info (ID) which is encrypted under the public key of reader to reader. Else the protocol is terminated.

A section of ownership transfer

(9) Server get the public key K1 of new group owner. Server transmit $Ek\,(ID \oplus Rt)$, $Rt \oplus K1$, $Ek\,(Rt)$ and Rr which is encrypted under the public key of reader to reader. Then update the public key of owner to $K1$ and stroe K as the the key of successful authentication of last time.

(10) Reader check whether the Rr is equal to the number it stored. If it is equal, do the next step. Else terminate the protocol.

(11) Reader transmit $Ek\,(ID \oplus Rt)$, $Ek\,(Rt) \oplus Rr$ and $Rt \oplus K1$ to tag.

(12) Tag get Rr by compute $Ek\,(Rt) \oplus Rr \oplus Ek\,(Rt)$ and check whether Rr equal to the random number it stroed. If it is not equal, terminate the protocol. Else it means that the reader is authenticated.

(13) Tag check whether $Ek\,(ID \oplus Rt)$ equal to it stored. if it is true, do the next step. Else terminate the protocol.

(14) Tag get the public key $K1$ of new group owner by comput $Rt \oplus K1 \oplus Rt$. Then update K to $K1$. The process of group owner transfer is finish.

Figure 1 shows the process of mutul anthentication. Figure 2 shows the process of group ownership transfer. This protocol can help resist the attack we mentioned above. This protocol can adapt to the capability of compution about tag. If tag has strong capability of compution, it can adopt hash or PKI Infrastructure. If tag has weak capability of compution, it can adopt xor instead of $Ek\,()$, but premise is public key of owener must large enough.

4. Analyzing Protocol with Ban Logic

BAN logic is a well-known authentication logic , which can prove whether a protocol can reach expected target and find some flaws in the protocol . Syntax and Semantics of BAN logic is shown as follows [6]:

$P \mid \equiv X$: P trusts the message X is true, P believes X.

$P \lhd X$: P received a message contains X, P sees X.

$P \mid \sim X$: P has transmitted a message contains X. P said X.

$P \mid \Rightarrow X$: P controls X.

(X) : X is fresh. X has not been transmitted in any message before.

$P \overset{K}{\leftrightarrow} Q$: P and Q communicate to each other with the shared key K. No one discovered K excpte P, Q or a third party trusted by P or Q.

$\{X\}_K$: It means that X is encrypted under K.

Rules of BAN Logic

(1) Message-meaning rule

Rule 1 : $P \mid \equiv P \overset{K}{\leftrightarrow} Q\,,\, P \lhd \{X\}K \vdash P \mid \equiv Q \mid \sim X$

(2) Nonce-verification rule

Rule 2 : $P \mid \equiv \#\{X\}\,,\, P \mid \equiv Q \mid \sim X \vdash P \mid \equiv Q \mid \equiv X$

(3) Jurisdiction rule

Rule 3 : $P \mid \equiv Q \mid \Rightarrow X, P \mid \equiv Q \mid \equiv X \vdash P \mid \equiv \mathrm{X}$

(4) Seeing rules

Rule 4 : $p \lhd (X, Y) \vdash P \lhd X$

Rule 5 : $P \lhd < X >_K \vdash P \lhd X$

Rule 6 : $P \mid \equiv P \overset{K}{\leftrightarrow} Q\,,\, P \lhd \{X\}_K \vdash P \lhd X$

(5) Freshness rule

Rule 7 : $P \mid \equiv \#\{X\} \vdash P \mid \equiv \#\{X, Y\}$

(6) Belief rules

Rule 8 : $P \mid \equiv X\,,\, P \mid \equiv Y \vdash P \mid \equiv (X, Y)$

Rule 9 : $P \mid \equiv (X, Y) \vdash P \mid \equiv \mathrm{X}$

Rule 10 : $P \mid \equiv Q \mid \equiv (X, Y) \vdash P \mid \equiv Q \mid \equiv X$

Rule 11 : $P \mid \equiv Q \mid \sim (X, Y) \vdash P \mid \equiv Q \mid \sim X$

In this process, we use A represents tag; B represents reader; S represent database server; KBS represents the shared key between B and S. The initial assumptions are as follows:

(1) $B \mid \equiv B \overset{K_{BS}}{\leftrightarrow} S$,

(2) $S \mid \equiv B \overset{K_{BS}}{\leftrightarrow} S$,

(3) $A \mid \equiv A \overset{K}{\leftrightarrow} S$,

(4) $A \mid \equiv A \overset{K}{\leftrightarrow} S$,

(5) $S \mid \equiv \#(A \overset{K}{\leftrightarrow} S)$,

(6) $A \mid \equiv \#(A \overset{K}{\leftrightarrow} S)$,

(7) $A \mid \equiv S \mid \Rightarrow A \overset{K}{\leftrightarrow} S$,

(8) $A \mid \equiv \#(R_t)$,

(9) $B \mid \equiv \#(R_r)$,

(10) $S \mid \equiv \#(R_s)$,

(11) $B \mid \equiv \#(Info(ID))$,

(12) $B \mid \equiv S \mid \Rightarrow Info(ID)$,

(13) $A \mid \equiv S \mid K_1$,

The idealization of the RFID protocol are as follows:

$B \rightarrow S : \{R_r\}_{K_{BS}}$
$S \rightarrow B : \{R_s, R_t\}_{K_{BS}}$
$B \rightarrow A : R_r$
$A \rightarrow B : \{R_t, ID\}_K$
$B \rightarrow S : \{R_s, \{R_t, ID\}_k\}_{K_{BS}}$
$S \rightarrow B : \{Info(ID)\}_{K_{BS}}$
$S \rightarrow B : \{R_r, \{R_t, ID, K_1\}_k\}_{K_{BS}}$
$B \rightarrow A : \{R_t, ID, K_1\}_k, R_r$

According to BAN Logic, the interpretation of the RFID protocol are as follows:

(14) $S \lhd \{R_r\}_{K_{BS}}$

(15) $B \lhd \{R_s, R_r\}_{K_{BS}}$

(16) $A \lhd R_r$

(17) $B \lhd \{R_t, ID\}_K$

(18) $S \lhd \{R_s, \{R_t, ID\}_k\}_{K_{BS}}$

(19) $B \lhd \{Info(ID)\}_{KBS}$

(20) $B \lhd \{R_r, \{R_t, ID, A \overset{K_1}{\leftrightarrow} S\}_k\}_{K_{BS}}$

(21) $A \lhd \{R_t, ID, A \overset{K_1}{\leftrightarrow} S\}_k, R_r$

The goals expected to achieve:

$B \mid \equiv Info(ID), A \mid \equiv S \overset{K}{\leftrightarrow} A$

Under the Rule 1, formula (19) and the assumption (1), we have

(22) $B \mid \equiv S \mid \sim Info(ID)$

Under the Rule 2, formula (22) and the assumption (11), we have

(23) $B \mid \equiv S \mid \equiv Info(ID)$

Under the Rule 3, formula (23) and the assumption (12), we have

$B \mid \equiv Info(ID)$

So the goal of $B \mid \equiv Info(ID)$ has been proved.

Under the Rule 1, formula (21) and the assumption (3), we have

(24) $A \mid \equiv S \mid \sim (R_t, ID, A \overset{K_1}{\leftrightarrow} S)$

Under the Rule 5 and assumption(8), we have

(25) $A \mid \equiv \#(R_t, ID, A \overset{K_1}{\leftrightarrow} S)$

Under the Rule 2, formula (24) and (25), we have

(26) $A \mid \equiv S \mid \equiv (R_t, ID, A \overset{K_1}{\leftrightarrow} S)$

Under the Rule 9 and formula (26), we have

(27) $A \mid \equiv S \mid \equiv A \overset{K_1}{\leftrightarrow} S$

Under the Rule 3, formula (27) and assumption (13), we have

$A \mid \equiv S \overset{K}{\leftrightarrow} A$

As shown in the above analysis, the protocol can achieve its goals.

5. The Improved Apriori Algorithm

The notion of the improved algorithm. The Boolean matrix is used to describe the transaction database. And the number '1' and '0' are used to replace the corresponding items. After this the Boolean matrix is used to count the support of the item sets in the database and need not scan the transaction database any more. According to the operation of vector, the Boolean matrix's components can be seen as row vectors and such improved algorithm just uses the "*and*" operation to count the support quickly on the Boolean matrix.

(1) First the transaction database needs to be converted into Boolean matrix. If the transaction database contained m items and n transactions the Boolean matrix will have $m + 1$ row and $n + 2$ columns. The first column registers "*items*" and the first row records "*TID*" of the transactions. The last column is used to record the support of the item sets. Second, the min-support is compared with the support of the item sets, if the support of the item sets is smaller than the min-support the row of the item sets will be deleted. By doing this the new Boolean matrix just contains the one-frequent item sets. And if it wants to know the *k*-frequent item sets, the "*AND*" operation will just be carried out on the k rows. Finally all the frequent item sets can be found out.

(2) Usually there are a large number of transactions in the transaction database, so the Boolean matrix is very large. And the algorithm is carried out on the Hadoop platform. According to the number of the DataNodes of the Hadoop, the Boolean matrix is divided into several parts based on the columns. And each part is located on each Hadoop DataNode. By doing this the algorithm can be executed parallel.

The description of the algorithm.

First input: the transaction database *D* and the min-support minsup.

The result output: all the frequent item sets in the database *D*.

The following is the description of the algorithm:

(1) [Convert the transaction database D to Boolean matrix DB]

DB = convert (database D, minsup);

If DB = NULL

End there is no frequent item set

Else

The 1-frequent item sets are the items which are the rows of the Boolean matrix

(2) [Divide the Boolean matrix into blocks]

If n is the number of the DataNodes of Hadoop Platform

Then the Boolean matrix DB is divided into n blocks, each having several columns of the matrix

(3) [Find all other frequent item sets]

$L1$ = the collection of items in the matrix DB is 1-frequent item sets

For k from 2 to the Max which is count of the rows of the matrix DB, execute

$Ck = GENCk(DB, Lk-1)$ [use the AND operation of matrix on any k rows of the DB]

$Lk = GENLk(DB, Ck-1, \text{minsup})$ [get the k-frequent item sets]

Then $L = L2 \cup L2 \cup ... \cup Lk-1 \cup Lk \cup ... \cup LMax$

(4) [Compute the confidence of the item sets to find the association]

(5) [END]

The first step of the algorithm is to convert the transaction database into Boolean matrix. The algorithm needs to scan the database once only. And in this step it can find the 1-frequent item sets and delete the non-frequent item sets. Next, the Boolean matrix is divided into several parts and each part is located on one DataNodes of Hadoop. The "*AND*" operation is carried out on the Boolean matrix to find the other frequent item sets.

5.1 The Performance Analysis of the Improved algorithm

The traditional apriori algorithm needs to scan the transaction database when it wants to know the candidates of the item sets. If n is the number of the transactions of database and m is the average length of item sets. So the traditional apriori algorithm needs to scan $O(n * m)$ time to find the first 1-frequent item sets. And the time $O(Lk-1 * Lk-1)$ to find the candidates Ck. To count the support needs time of $O(n * Ck)$.

The improved apriori algorithm in this paper needs to scan the transaction database one time. And the first time to scan the database can find the 1-frequent item sets and can exclude the non-useful item sets. In the following steps we just use the "*AND*" operation of matrix to find other frequent item sets. And it need not scan the original database. Because of the high degree parallelism of the Hadoop, the time consumed in counting the support should be cut down. The time is only one in n(there are n DataNodes of Hadoop).

5.1.1 Case analyze

Assume that D be a transaction database and $D = \{T1, T2, T3, \ldots, Tn\}$. There n is the number of the transaction. And I is a set of items and $I = \{I0, I1, I2, \ldots, Im\}$, There m is the number of the items.

According to the property the Boolean matrix is used to describe the transaction database. First the transaction database's data format is vertical data format as table 1.

Item	TID
$I0$	$T1, T2, T4$
$I1$	$T1, T2, T4$
$I2$	$T1, T2, T3$
$I3$	$T3$
$I4$	$T1, T4$

Table 1. Vertical data format of transaction database

Second, the transaction database is scanned for one time and is converted to Boolean matrix. If the transaction in the database has the items, the Boolean value in the Boolean matrix is noted '1'; otherwise the value is '0'. Table 2 is the Boolean expression of the transaction database

Item	TID				Support
	$T1$	$T2$	$T3$	$T4$	
$I0$	1	1	0	1	3
$I1$	1	1	0	1	3
$I2$	1	1	1	0	3
$I3$	0	0	1	0	1
$I4$	1	0	0	1	2

Table 2. Boolean matrix of the transaction database

Assume the minsup = 3. It deletes the items whose support is less than the minsup in the Boolean matrix. Table 3 is the new Boolean matrix.

Item	TID				Support
	$T1$	$T2$	$T3$	$T4$	
$I0$	1	1	0	1	3
$I1$	1	1	0	1	3
$I2$	1	1	1	0	3

Table 3. The new Boolean matrix

In table 3, there are three frequent 1-items $I0$, $I1$, and $I2$. And the frequent item sets are made up of the three items. So the largest frequent items are composed up to three items. Next we divide table 3 into blocks according to the number of the DataNodes of Hadoop. Suppose that there

are two DataNodes, it is divided into two blocks by column. For example, the blocks are as in table 4. DataNode1 holds the block1 and the DataNode2 holds the block2. In each DataNode the Boolean matrix can be seen as the row-vectors as $I0 = \{1, 1, 0,1\}$, $1 = \{1, 1, 0, 1\}$, $I2 = \{1, 1, 1, 0\}$. If it wants to know the frequent 2-items just get them by phase and get the sum.

Item	TID		Support
	$T1$	$T2$	
$I0$	1	1	3
$I1$	1	1	3
$I2$	1	1	3

Item	TID		Support
	$T3$	$T4$	
$I0$	0	1	3
$I1$	0	1	3
$I2$	1	0	3

Table 4. The two blocks_block1 blocks_block2

Since there are three frequent 1-items I_0, I_1, I_2, the frequent 2-items can be $\{I_0, I_1\}$, $\{I_0, I_2\}$ and $\{I_1, I_2\}$. Therefore the support of $\{I_0, I_1\}$ is $I_0 \odot I_1 = \{1, 1\} \odot \{1, 1\} + \{0, 1\} \odot \{0, 1\} = 3$. So $\{I_1, I_2\}$ is frequent 2-items. As the same the supports of $\{I_0, I_2\}$ and $\{I_1, I_2\}$ are 2, they are not the frequent 2_items. The support of 3-items $\{I_0, I_1, I_2\}$ is $I_0 \odot I_1 \odot I_2 = \{1, 1\} \odot \{1, 1\} \odot \{1, 1\} + \{0, 1\} \odot \{0, 1\} \odot \{1, 0\} = 2$. Thence it is not the frequent 3-items. Finally it can get all the frequent item sets $\{\{I_0\}, \{I_1\}, \{I_2\}, \{I_0, I_1\}\}$. The meaning of the symbol $\odot$ is to compute the support of the item sets. It counts the support by adding the summation of the vector by bitwise. In each DataNode of Hadoop the operations is run at the same time.

6. Conclusions

It is a chanllenge to design an RFID protocol with ownership transfer because RFID system have some defect innately.This paper propose an RFID protocol which can be implemented in either high-cost tags or low-cost tags. This protocol can be considered as safe by stipulation of analyzing methods of BAN Logic.

References

[1] Chien, H. Y., Chen, C. H. (2007). Mutual authentication protocol for RFID conforming to EPC Class1 Generation 2 standards, *Computer Standards & Interfaces*, 29 (2) 254-259, February.

[2] Chih-Hung Wang, Shan Chin. (2009). A new RFID Authentication protocol with ownership transfer in an Insecure communication enviroment, 2009 Ninth *International Conference on Hybrid Intelligent Systems*, p . 486-491.

[3] Osaka, K., Takagi, T., Yamazaki, K., Takahash, O. (2006). An Efficient and Secure RFID Security Method with Ownership Transfer, *Computational Intelligence and Security*, 2, p. 1090-1095.

[4] Lei, H., Cao, T. (2007). RFID Protocol enabling Ownership Transfer to protect against Traceability and Dos attacks, The First International Symposium on Data, *Privacy and E-Commerce* (ISDPE 2007). 1-3, p. 508-510, Nov.

[5] Tripathy, S., Nandi , S. (2006). Robust Mutural Authentication for Low cost RFID Systems, 2006 *IEEE International Conference on Industrial Informatics,* p. 949-954, Aug.

[6] Kernal Bicakci, Nazife Baykal. (2003). One-Time Passwords:Security Analysis Using BAN Logic and Integrating with Smartcard Authentication. *Lecture Notes in Computer Science*, p. 794-801.