I. J. Computer Network and Information Security, **2015, 4, 44-53**
Published Online March 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.04.06

Object Authentication Using RFID Technology: A Multi-tag Approach

Subhasish Dhal
Indian institute of Technology Kharagpur, 721302, India
Email: sdhal@cse.iitkgp.ernet.in

Indranil Sen Gupta
Indian institute of Technology Kharagpur, 721302, India
Email: isg@iitkgp.ac.in

Abstract—Authentication is an important requirement in various applications to restrict the non-legitimate access to certain resources. Radio Frequency Identification (RFID) technology helps to perform the authentication task. The detection probability of an object during the authentication process can be increased using multiple number of RFID tags in the object. However, many security risks such as eavesdropping, location privacy etc. are involved in this technology. This paper proposes a secure and lightweight authentication scheme assuming the objects are attached with multiple number of RFID tags. Proper analysis has been carried out to evaluate the security of the proposed scheme, including comparison with a few existing schemes in terms of computation, communication and storage requirements.

Index Terms—Authentication, Detection probability, Multi-tag, RFID, Security.

I. INTRODUCTION

In RFID technology, a small chip (RFID tag) contains identification information of an object and this information is read by the RFID reader in order to identify the object. Hence, this technology is useful in many real life applications. For example, the items in a shopping mall can be attached with RFID tag and be identified with the help of RFID reader. However, an unauthorized person can access the tag attached to an item and decrease the cost of the item. Therefore, authentication is an important requirement for the applications based on RFID technology[1][2]. Traditionally, the objects are attached with single RFID tag. However, the position of the object where the tag is attached may not be detectable by the reader whereas some other positions of the same object are detectable. Therefore, the detection probability of an object in this arrangement is less [3]. The detection probability of the object can be increased using multiple number of tags [3]. The tags are attached in such a way that if any part of the object is within the communication range of the reader, there is at least one tag attached to the object that is within the communication range of the reader. Thus the detection probability of the object increases [3]. Many security issues are involved in RFID technology such as eavesdropping, location privacy etc.[4] However, classical cryptography techniques are not applicable to this environment since the RFID tag has low resources in terms of computation, communication and storage. Hence we require lightweight cryptography primitives to make a balance between security and resource requirement. The researchers in earlier authentication schemes concentrated on the balance between security and resource optimization. However, these schemes cannot be extended to multi-tag environment since they use single set of security information for an object. If the same information is copied to multiple tags attached to the object, the adversary can easily compromise all the tags by compromising any one tag attached to the object. This motivates to do further research in this area.

The research questions that have been addressed in this paper are: 1) Whether multiple resources can be utilized to enhance the security. 2) Whether it is possible to prevent possible attacks during the authentication process. 3) Whether it is possible to implement the authentication task amid the resource limitations. The objective of this paper is to design an authentication scheme in multi-tag environment which can make a balance between the security and resource requirement. In addition to this, we have to find any benefit of multiple number of tags in an object. This paper proposes a lightweight authentication scheme assuming the objects are attached with multiple number of RFID tags. The proposed scheme utilizes multiple number of tags to increase the difficulty for the adversary and it can prevent most of the attacks. Proper analysis has been carried out to evaluate the security and resource requirements of the proposed scheme. Rest of the paper is organized as follows. In Section II, we have analyzed a few existing authentication schemes [5][6][11][12][14]. Section III describes the proposed authentication scheme. In Section IV, we have analyzed the proposed authentication scheme and then we have concluded in Section V.

II. RELATED WORKS

Many authentication schemes exist in the literature. However, the existing schemes consider single RFID tag for each object. In this section, we revisit a few authentication schemes [5][6][11][12][14] and analyze their limitations.

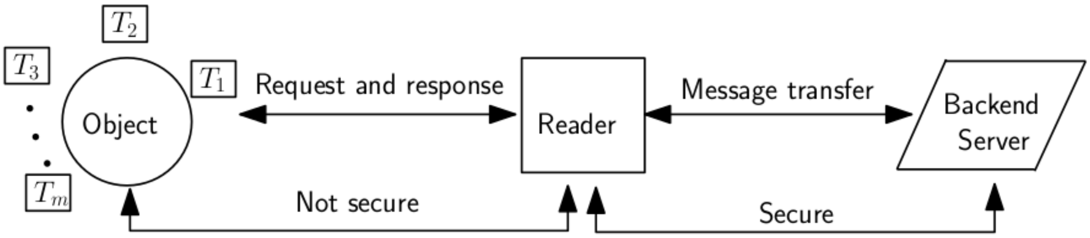

Fig. 1. Communication model

The scheme proposed by Weis et al.[5] is a hash function bashed authentication scheme. This scheme is vulnerable to many attacks like traceability, replay attack, etc. The modified version of this scheme called randomized hash-lock scheme [5] resolves the location privacy problem. However, it cannot prevent other kinds of attacks. Other hash function based authentication schemes are presented in [6][7][8][9][10]. Since these schemes use hash function, the tag efficiency is low. Guo Rui Li et al. [11] proposed an authentication scheme based on public key cryptography that can prevent many attacks. However, the use of public key cryptography makes their scheme computationally infeasible on RFID platform. Kim and Jun [12] proposed a lightweight mutual authentication protocol. The limitation in their scheme is that it can detect any attack at the last phase of the authentication process which costs unnecessary computations before the detection. Song and Mitchell [12] have proposed an authentication scheme which suffers from high computation overhead due to hash and MAC operations. Some attacks against this scheme are also reported in [13].

According to the research findings in [3], the attachment of multiple number of tags to an object helps to increase the detection probability of the object. However, to the best of our knowledge, any authentication scheme based on this multi-tag concept has not yet been reported in the literature. Our work in [14] focuses the multi-tag concept. In this protocol, at least the threshold number of tags attached to an object which were authenticated successfully in a particular session needs to be visible to the reader in order to successful authentication of the object in the next session. The proposed scheme in this paper although used multiple tags in an object, it does not have this limitation. In addition to this, a proper analysis of the improved scheme has been carried out which were missing in [14].

III. Proposed Scheme Using Multi-tag RFID System

We propose an efficient authentication scheme in this paper which assumes that every object is attached with multiple number of tags. Before describing the proposed scheme we describe the Communication Model and the Threat Model. Table 1 lists the meaning of symbols used in the following discussions.

Table 1. Meaning Of Symbols

Symbol	Meaning
G_j	An object
m	Number of tags attached to an object
T_i	i^{th} tag in an object
IN_i	Index value
S_i	Secret key
TID_i	Tag id in tag memory
N_i	Session key in tag memory
$TID_{i,old}$	Old tag id in backend server
$TID_{i,new}$	New tag id in backend server
$N_{i,old}$	Old session key in backend server
$N_{i,new}$	New session key in backend server
U_i	Update status
V, g_i, g_i'	Random numbers
$Valid_j$	Validity information for G_j

A. Communication Model

The components involved in the communication model are a set of objects, RFID reader and a trusted server called backend server. Every object is attached with m number of RFID tags in a process similar to [3]. A workstation acts as the backend server which has relatively higher storage capacity. It keeps the information of the objects. A RFID reader acts as an intermediary between the tags attached to the objects and the backend server. The communication between the reader and the backend server is wired or wireless and is assumed to be secured. On the other hand, the communication between the reader and the tags attached to the objects are wireless and is not secure. Fig. 1 illustrates this communication model.

B. Threat Model

He adversaries may utilize the insecure medium between the reader and the tags attached to the objects. Following are the possible attacks which can be mounted during the authentication process.

Passive attacks: The adversary $\mathcal{A}$ silently extracts secret information about the legitimate objects.

- *Eavesdropping:* A silently listens to the communication and tries to extract the secret information such as identifier, session key, secret key, etc.
- *Location privacy:* A tries to find out a pattern from the requests and responses, and tries to trace the object.
- *Location privacy between two successful sessions:* Between two consecutive successful sessions, A can try to trace an object.

Active attacks: The adversary not only listens to the vital information but also tries to disrupt the authentication process. Any adversary may mount the following active attacks:

- *Man-in-the-middle attack:* A may modify the information communicated through insecure medium and thus can disrupt the authentication process.
- *Replay attack:* The authentication information of a legitimate session may be saved and replayed for successful validation in later sessions.
- *Forward secrecy and Backward secrecy:* Compromising the secret information used in one valid session, A may try to obtain the secret information to be used in later or previous sessions.
- *De-synchronization attack:* In some situations, the information such as identifier, session key etc. for an object are updated and then communicated from either reader to object or object to reader in each successful session. However, if an adversary blocks the updated information then there can be a synchronization problem between backend server and the object.
- *Impersonation attack:* A may clone a legitimate tag and use the cloned tag to impersonate the legitimate tag.

C. Proposed protocol

The proposed authentication scheme has two phases, namely, Setup phase and Authentication phase. Fig. 3 illustrates these phases. Before introducing these phases, we describe the information maintained by the components mentioned in the communication model.

Information in Backend Server and Tags: The tag attached to an object contains the information about the object. It contains the index value IN_i, secret key S_i, tag identifier TID_i and session key N_i.

IN_i	S_i	TID_i	N_i

The backend server contains a database to keep the information for all the objects. One record in the database contains the information about one object. This record contains a validity information valid j and the information for m number of tags attached to the corresponding object.

The record for an object is divided into *m* number of sub-records. Each sub-record contains index value IN_i, secret key S_i, two tag identifiers $TID_{i,old}$, $TID_{i,new}$, two session keys $N_{i,old}$, $N_{i,new}$, update status U_i and random number information g_i'. Fig. 2 illustrates the record for an object kept in the backend server.

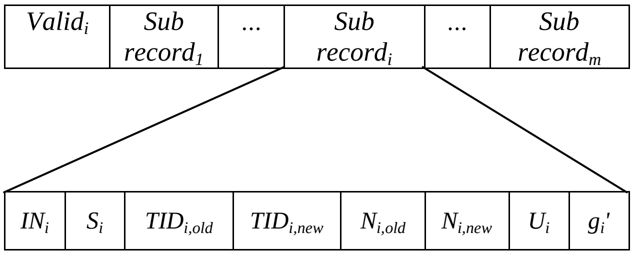

Fig. 2: Information in backend server

Setup phase: In Setup phase, the tags and the backend server are initialized and deployed for authentication process to be performed in future. We consider *n* objects. In the illustration, we describe the initialization process for the object G_j, $1 \le j \le n$.

- G_j is assigned the tags T_i, i = 1, 2, …, *m*. The memory of each tag T_i is loaded with an index value IN_i (Index values are unique corresponding to the tags attached to an object. However, any two or more objects have the tags with same index value.), a secret key S_i, a tag id TID_i and a session key N_i.
- The $Valid_j$ field in the record for G_j is initialized to zero. The sub-records for the tags attached to G_j are initialized as follows. The index value IN_i and secret key S_i which were loaded to the memory of the tag T_i are also loaded to the corresponding fields. The tag id TID_i which was loaded to the memory of tag T_i are also loaded to both the fields $TID_{i, old}$ and $TID_{i, new}$. Similarly, the session key N_i which was loaded to the memory of the tag T_i are also loaded to both the fields $N_{i, old}$ and $N_{i, new}$.

Thus, after initialization process, the assigned tags are attached to the corresponding objects appropriately similar to the process described in [1] and the objects are deployed.

Authentication phase: In authentication phase, the objects are authenticated as and when required. We use separate algorithms for the components mentioned in the communication model (described in Section III.A). Algorithms 1, 2, 3 are performed by the reader, the tags attached to an object and the backend server respectively.

Brief description: During authentication phase, the backend server generates a random number v and sends it to the reader. The reader broadcasts this *v*. The tags within the communication range of the reader receive this *v* and replies with authentication information K_i along with random number g_i and index value IN_i. Reader receives the responses from the tags and forwards these to the backend server. The backend server receives each set of response IN_i, K_i, g_i and verifies the validity. It starts with the first record kept in the database and uses the sub-record under this record having index IN_i. It verifies K_i using the new identifier and session key and on successful verification, it makes the corresponding update flag U_i as 1. If verification is not successful using new information, it uses old identifier and session key to verify K_i. This time it makes the update flag U_i as 2. It also increases $valid_j$ by 1 on successful verification using either new or old information. If the verification fails using both new and old information, it selects the next record and continues this until it finds a valid record or finishes with all records in the database.

Object	Reader	Backend Server
Setup phase		
IN_i, S_i, TID_i, N_i $i = 1, 2, ..., m$		$IN_i, S_i, TID_{i,old}, TID_{i,new}, N_{i,old}, N_{i,new}$ $U_i, g_i', i = 1, 2, ..., m, Valid_j \leftarrow 0$
Authentication phase		
	← 2. v ← 1. v	Generates v
$K_i = (TID_i - g_i) \oplus ((v \oplus g_i) - N_i)$	3. IN_i, K_i, g_i → 4. IN_i, K_i, g_i →	Verifies K_i with j^{th} record under index IN_i If verified on $TID_{i,new}, N_{i,new}$ $Valid_j \leftarrow Valid_j + 1, U_i \leftarrow 1, g_i' \leftarrow g_i$ Else if verified on $TID_{i,old}, N_{i,old}$ $Valid_j \leftarrow Valid_j + 1, U_i \leftarrow 2, g_i' \leftarrow g_i$ If $Valid_j \geq l, j = 1, 2, ..., n$ If $U_i = 1, i - 1, 2, ..., m$ Generates TID_i', N_i' randomly Generates P_{1i}, P_{2i}, P_{3i} using $TID_{i,new}$, $N_{i,new}, TID_i', N_i', g_i', v$ $TID_{i,old} \leftarrow TID_{i,new}, N_{i,old} \leftarrow N_{i,new}$ $TID_{i,new} \leftarrow TID_i', N_{i,new} \leftarrow N_i'$ Else If $U_i = 2$ Generates TID_i', N_i' randomly Generates P_{1i}, P_{2i}, P_{3i} using $TID_{i,old}$, $N_{i,old}, TID_i', N_i', g_i, v$ $TID_{i,new} \leftarrow TID_i', N_{i,new} \leftarrow N_i'$ Else ignores and stops.
Extracts TID_i', N_i' from P_{1i}, P_{2i} If P_{3i} is valid Updates $TID_i \leftarrow TID_i', N_i \leftarrow N_i'$	← 6. $IN_i, P_{1i}, P_{2i}, P_{3i}$ ← 5. $IN_i, P_{1i}, P_{2i}, P_{3i}$	

Fig. 3: Proposed authentication protocol

Algorithm 1 executed by reader

1: Receives v from backend server and broadcasts
2: Receives computed information IN_i, K_i, g_i from tags
3: Forwards IN_i, K_i, g_i to backend server
4: Receives computed information IN_i, P_{1i}, P_{2i}, P_{3i} from backend server
5: Forwards IN_i, P_{1i}, P_{2i}, P_{3i} to tags

Thus the backend server verifies all the responses. It then identifies the valid object. To do this, it searches the records with $valid_j$ greater than or equal to the threshold value l. If it finds any such record, it identifies the corresponding object and generates the update information P_{1i}, P_{2i}, P_{3i} for the tags T_i attached to the same object for which the U_i is a nonzero value. If the value of U_i is 1, it uses the new identifier $TID_{i,new}$ and

Algorithm 2 executed by a tag attached to an object

1: Receives random number v
2: Generates g_i randomly and then computes $K_i \leftarrow (TID_i - g_i) \oplus ((v \oplus g_i) - N_i)$
3: Sends IN_i, K_i, g_i to reader
4: Receives IN_i, P_{1i}, P_{2i}, P_{3i} from reader
5: **If** IN_i = own index **then**
6: $TID_i' \leftarrow ((P_{1i} \oplus ((TID \oplus v) - S_i)) - S_i) \oplus g_i$, $N_i' \leftarrow ((P_{2i} \oplus ((N_i \oplus g_i) - S_i)) - S_i) \oplus v$
7: **If** $P_{3i} = ((S_i \oplus v) - (P_{1i} \oplus TID_i' \oplus N_i)) \oplus ((P_{2i} \oplus TID_i \oplus N_i') - (S_i \oplus v))$ **then**
8: Updates $TID_i \leftarrow TID_i', N_i \leftarrow N_i'$

session key $N_{i,new}$ to generate the update information. Otherwise, it generates the update information using the old identifier $TID_{i,old}$ and session key $N_{i,old}$. After completing the updation process, it resets the valid flags $valid_j$ of all the objects and update flags U_i of all the tags kept in the database. The backend server sends IN_i, P_{1i}, P_{2i} and P_{3i} to tags via reader. The tag receives this

Algorithm 3 executed by backend server

Generates and sends a random number v to reader
Receives IN_i, K_i, g_i from reader
For all IN_i, K_i, g_i
  $j \leftarrow 1$
  $Satisfy \leftarrow 0$
  Repeat
    Selects Information kept under index IN_i in j^{th} record
    If $K_i = [(TID_{i,new} \oplus g_i) - ((v \oplus g_i) \oplus N_{i,new})]$ **then**
      $valid_j \leftarrow valid_j + 1$, $U_i \leftarrow 1$, $g_i' \leftarrow g_i$, $Satisfy \leftarrow 1$
    ElseIf $K_i = [(TID_{i,old} \oplus g_i) \oplus ((v \oplus g_i) \oplus N_{i,old})]$ **then**
      $valid_j \leftarrow valid_j + 1$, $U_i \leftarrow 2$, $g_i' \leftarrow g_i$, $Satisfy \leftarrow 1$
    $j \leftarrow j + 1$
  Until $j > n$ **or** $Satisfy = 1$
For $j = 1$ **to** n
  If $valid_j \geq l$ **then**
    This object is authenticated
    For $i = 1$ **to** m
      If $U_i = 1$ **then**
        Randomly generates TID_i', N_i'
        Computes $P_{1i} \leftarrow (S_i + (TID_i' \oplus g_i')) \oplus ((TID_{i,new} \oplus v) - S_i)$,
        $P_{2i} \leftarrow (S_i + (N_i' \oplus v)) \oplus ((N_{i,new} \oplus g_i') - S_i)$,
        $P_{3i} \leftarrow ((S_i \oplus v) - (P_{1i} \oplus TID_i' \oplus N_{i,new})) \oplus ((P_{2i} \oplus TID_{i,new} \oplus N_i) - (S_i \oplus v))$
        Sends IN_i, P_{1i}, P_{2i}, P_{3i} to reader
        Updates $TID_{i,old} \leftarrow TID_{i,new}$, $N_{i,old} \leftarrow N_{i,new}$, $TID_{i,new} \leftarrow TID_i'$, $N_{i,new} \leftarrow N_i'$
      Else If $U_i = 2$ **then**
        Randomly generates TID_i', N_i'
        Computes $P_{1i} \leftarrow (S_i + (TID_i' \oplus g_i')) \oplus ((TID_{i,old} \oplus v) - S_i)$, $P_{2i} \leftarrow (S_i + (N_i' \oplus v)) \oplus ((N_{i,old} \oplus g_i') - S_i)$,
        $P_{3i} \leftarrow ((S_i \oplus v) - (P_{1i} \oplus TID_i' \oplus N_{i,old})) \oplus ((P_{2i} \oplus TID_{iold} \oplus N_i) - (S_i \oplus v))$
        Sends IN_i, P_{1i}, P_{2i}, P_{3i} to reader
        Updates $TID_{i,new} \leftarrow TID_i'$, $N_{i,new} \leftarrow N_i'$
For $j = 1$ **to** n
  $valid_j \leftarrow 0$
  For $i = 1$ **to** m
    $U_i \leftarrow 0$

information and updates its memory after verifying the received information.

IV. Analysis of the Proposed Scheme

We analyze the proposed scheme to evaluate its applicability in practical scenarios. We choose four parameters, namely, security, computation, communication and storage requirements.

A. Security Analysis

The communication between tag and the reader can be misused by the adversaries who may try to mount various attacks. Therefore the proposed scheme needs to be secure against these attacks. We analyze the security of the proposed scheme in this section.

Informal Security Analysis: We informally analyze how an adversary $\mathcal{A}$ can mount various attacks mentioned in the threat model and how the proposed scheme can prevent these attacks.

- *Eavesdropping:* A can intercept g_i, v, K_i, P_{1i}, P_{2i}, P_{3i} and try to find out the secret information such as secret key S_i, session key N_i, etc. For example, he may try to compute TID_i from K_i. He needs to separate $(TID_i - g_i)$ and $((v \oplus g_i) - N))$ from K_i and then can compute TID_i from $(TID_i - g_i)$. However, Shannon has proved in [15] that it is not possible to separate A and B from $A \oplus B$ as long as the bit size of A and B are same and any of A or B does not contain a value which it had contained in any other session completed earlier[1]. Since the size of $(TID_i - g_i)$ and $((v \oplus g_i) - N))$ are same and they are not same in multiple sessions, A is unable to separate these from K_i. Similarly, the other equations are secure from eavesdropping.
- *Location privacy:* A can try to find out a pattern using the information g_i, v, K_i, P_{1i}, P_{2i}, P_{3i} in multiple sessions. The proposed scheme uses new random numbers in each session to generate g_i, v, K_i, etc. For example, K_i consists of randomly generated g_i and v which were not used in the previous sessions. Therefore the adversary cannot relate the K_i of one session with the K_i of other sessions. Similarly, he cannot use other information transmitted through the insecure medium to find a pattern. He can try to use the index information to trace an object. However, there can be the responses with same index information from more than one object.
- *Location privacy between two successful sessions:* During the time between two successful sessions, A can try to replay same v and can expect same response K_i from the tag. However, the tag randomly generates g_i and includes it into K_i. Therefore, the responses are not same and A cannot trace the object. In similar argument, he cannot trace the object intercepting the information P_{1i}, P_{2i}, P_{3i}.

[1] For i^{th} bit, $C_i = A_i \oplus B_i$. Let B_i is a random bit. Hence for all i, $P(B_i = 0) = P(B_i = 1) = 0.5$. Let $P(A_i = 0) = p_i$. Therefore, $P(A_i = 1) = 1 - p_i$. Now, $P(C_i = 0) = P(A_i = 0) \times P(C_i = 0 \mid A_i = 0) + P(A_i = 1) \times P(C_i = 0 \mid A_i = 1) = P(A_i = 0) \times P(B_i = 0) + P(A_i = 1) \times P(B_i = 1) = pi \times 0.5 + (1 - p_i) \times 0.5 = 0.5$. Therefore, $P(C_i = 0)$ does not depend on p_i. Conversely, we can say that the probability of obtaining correct A_i from the given C_i is 0.5, where B_i is random.

- *Man-in-the-middle attack:* A can modify K_i and expect that the modified information will be validated in the backend server. However, since he does not know the secret information, his modified information cannot be validated successfully. A can modify P_{1i}, P_{2i} and expect that the tag will extract the wrong information from P_{1i}, P_{2i} and update. However, since he does not know the secret information, he cannot generate a valid P_{3i} which can validate the modified P_{1i} and P_{2i}. The tag will use this P_{3i} to verify the authentication and integrity of P_{1i} and P_{2i}, and will ignore the modified information.
- *Replay attack:* A can replay v used in the previous session and can expect that the tag will send the same response K_i. Since the tag uses a random number g_i as we have mentioned in the argument of location privacy during the time between two successful sessions, A cannot trace the object. He can replay the K_i. However, the v used in this K_i is not equal to the v generated in this session by the backend server. Therefore, the replayed information cannot be validated in the backend server. Similarly, the replayed P_{1i}, P_{2i} and P_{3i} cannot be validated in the tag due to new g_i and v.
- *Forward secrecy:* Suppose A captures TID_i and try to compute TID_i'. Since he does not know S_i, he is unable to compute $((TID_i \oplus v) - S_i)$ from P_{1i} and hence cannot compute TID_i'. In similar argument, he cannot compute N_i' using N_i. If he is able to capture Si, then also he cannot compute TID_i' or N_i' since he does not know TID_i. If he is able to capture all S_i, N_i and TID_i, then only he can compute TID_i' or N_i'.
- *Backward secrecy:* Similar to forward secrecy, the proposed scheme prevents the backward secrecy, i.e A can only be able to intercept S_i, N_i and TID_i if he is able to capture all the secrets S_i, TID_i' and N_i.
- *De-synchronization attack:* A tries to mount this attack as following:
  - Blocks the update information P_{1i}, P_{2i}, P_{3i} and expects that the backend server has modified the session key and tag id, however, the tag has not updated the corresponding secrets and they cannot communicate in future. The proposed scheme keeps the old copy of the tag id and session key. Therefore, the response from the tag can be validated in backend server using the old information and this information is unchanged until the backend server finds that the tag has updated its information, i.e. the response from the tag has verified using new information.
  - Modifies P_{1i}, P_{2i} and expects that the tag retrieves the wrong information and hence there will be a mismatch between the information in tag and the backend server. As we have explained in the Man-in-the-middle attack, the tag will update only if it verifies P_{3i} successfully which is the integrity information of P_{1i}, P_{2i}. Hence tampering of P_{1i}, P_{2i} will be detected and the tag will not update the secrets. Therefore, the proposed scheme prevents the De-synchronization attack and the tag and the backend server can still be able to communicate further after this attack.
- *Impersonation attack:* $\mathcal{A}$ may physically clone a legitimate tag and use the cloned tag to impersonate the corresponding object. The proposed scheme uses a threshold value (l) to validate an object, i.e. $\mathcal{A}$ have to clone at least the threshold number of tags in order to impersonate an object. This will increase the difficulty for $\mathcal{A}$ to mount this attack. Thus the existence of multiple number tags in an object helps to increase the difficulty for the adversary. The proposed scheme has taken this advantage to increase the security during authentication.

Formal Security Analysis: In this section, we provide formal proofs which can assure the security of the proposed scheme. Firstly, we show that the adversary is unable to mount any attack by intercepting information transmitted through insecure medium during a particular session. Secondly, the adversary may try to intercept information transmitted during multiple sessions and try to mount attacks after manipulation of these information. We show that the proposed scheme is safe from this operation. Finally, we show that the adversary may try to approximate the addition or subtraction operation used in the equations for the information transmitted through insecure medium into XOR operation and try to mount attacks described in the threat model. We show that the probability of such attack in the proposed scheme is negligible.

Definition 1: (*Security of the Object Authentication Scheme* (*OAS*)). The OAS is secure if, any efficient adversary, given any one interaction (not necessarily complete) and a history of earlier interactions, cannot derive (with probability greater than $0.5 + \theta$, for a non-negligible θ) any secret.

Problem 1: Find p and q from a given number n, where p, q are unknown random numbers of same length (bit size) and $n = p \oplus q$.

Hardness of Problem 1: Let Adv_A^{XOR} denotes an adversary $\mathcal{A}$'s advantage in finding p and q from the given n, we have $Adv_A^{XOR} = \Pr[(p,q) \Leftarrow_R \mathrm{A} : p,q$ being random numbers of same length and $n = p \oplus q$[2]**]**. $\mathcal{A}$ is allowed to be probabilistic and the probability in the advantage is computed over the random choices made by $\mathcal{A}$. We call the Problem 1 as computationally infeasible, if $Adv_A^{XOR} \leq \in$, for any sufficiently small $\in \geq 0$.

Theorem 1: *The proposed object authentication scheme (OAS) is secure from intercepting the secret*

[2] $(x,y) \Leftarrow_R A$ denotes pair (X, Y) is selected randomly by the adversary $\mathcal{A}$.

information by $\mathcal{A}$ under the experiment depicted in Algorithm 4.

Algorithm 4: $EXP_A^{OAS}1$

1: Intercepts g_i, v, K_i, P_{1i}, P_{2i}, P_{3i}
2: Calls Disclose on input K_i and obtains $(TID_i - g_i)$, $((v \oplus g_i) - N_i) \leftarrow$ Disclose(K_i)
3: Computes $TID_i \leftarrow (TID_i - g_i) + g_i$, $N_i \leftarrow -(((v \oplus g_i) - N_i) - (v \oplus g_i))$
4: Calls Disclose on input P_{1i} and obtains $(S_i + (TID_i' \oplus g_i))$, $((TID_i \oplus v) - S_i) \leftarrow$ Disclose(P_{1i})
5: Computes $S_i \leftarrow -(((TID_i \oplus v) - S_i) - (TID_i \oplus v))$, $TID_i' \leftarrow (S_i + (TID_i' \oplus g_i)) - S_i) \oplus g_i$
6: Calls Disclose on input P_{2i} and obtains $(S_i + (N_i' \oplus v))$, $((N_i \oplus g_i') - S_i) \leftarrow$ Disclose(P_{2i})
7: Computes $N_i' \leftarrow ((S_i + (N_i' \oplus v)) - S_i) \oplus v$
8: **If** $P_{3i} = ((S_i \oplus v) - (P_{1i} \oplus TID_i' \oplus N_i)) \oplus ((P_{2i} \oplus TID_i \oplus N_i) - (S_i \oplus v))$ **then**
9: Successfully eavesdrop the secrets
10: **Else**
11: Return 0 (Failure)

Proof: A intercepts g_i, v, K_i, P_{1i}, P_{2i}, P_{3i} and tries to intercept the secret like session key, secret key, etc. using the experiment depicted in Algorithm 4. He calls a random oracle Disclose and finds the components tied with XOR operation. He then computes the secrets. However, the probability that he can separate the components tied with XOR operation depends on probability that he can solve the Problem 1. According to the hardness of the Problem 1, the probability of separating the components tied by XOR operation is sufficiently small. Therefore, the success probability of the experiment depicted in Algorithm 4 is sufficiently small and the proposed scheme is secure under this experiment.

Corollary 1: *The proposed object authentication scheme is secure from the attacks described in the Threat model.*

We define a random oracle Disclose.

Disclose: This random oracle unconditionally outputs p, q from the input n, where $n = p \oplus q$.

Proof: Suppose, A intercepts the secret information such as session key, id, etc. using the experiment depicted in Algorithm 4. Since he has the secret information, he can mount the attacks like replay attack, man-in-the-middle attack, de-synchronization attack. He further intercepts the information communicated in the next session and tries to mount the attack against the location privacy using the experiment depicted in Algorithm 5. He can also get the confirmation about the attack against forward and backward secrecy from this experiment. However, the success probability of this experiment depends on the probability of intercepting the various secrets. Therefore the success probability of this experiment depends on the probability of success in the experiment depicted in Algorithm 4 which is sufficiently small.

Algorithm 5: $EXP_A^{OAS}2$

1: Intercepts $g_i^1, v^1, K_i^1, P_{1i}^1, P_{2i}^1, P_{3i}^1$
2: **If** $K_i^1 = (TID_i' - g_i^1) \oplus ((v^1 \oplus g_i^1) - N_i')$ **then**
3: Tracing is successful
4: Computes $TID_i'' \leftarrow (P_{1i}^1 \oplus ((TID_i' \oplus v^1) - S_i) - S_i) \oplus g_i^1$
5: Computes $N_i'' \leftarrow (P_{2i}^1 \oplus ((N_i' \oplus g_i^1) - S_i) - S_i) \oplus v^1$
6: **If** $P_{3i}^1 = ((S_i \oplus v^1) - (P_{1i}^1 \oplus TID_i'' \oplus N_i')) \oplus ((P_{2i}' \oplus TID_i' \oplus N_i'') - (S_i \oplus v^1))$ **then**
7: Breaking forward secrecy is successful

Theorem 2: *The proposed object authentication scheme is secure from $\mathcal{A}$ under the experiment depicted in Algorithm 6.*

Algorithm 6 $EXP_A^{OAS}3$

1: **For** each pair of equations in $\mathcal{L}$
2: **If** the pair has common component **then**
3: Apply XOR operation on the pair and obtain a new equation $\mathcal{E}$
4: **If** $\mathcal{E} \notin \mathcal{L}$ **then**
5: Add $\mathcal{E}$ into $\mathcal{L}$
6: **End For**

Equations in unsuccessful session Ses_i

$$K_i = (TID_i - g_i) \oplus ((v \oplus g_i) - N_i) \quad (1)$$
$$P_{1i} = (S_i + (TID_i' \oplus g_i)) \oplus ((TID_i \oplus v) - S_i) \quad (2)$$
$$P_{2i} = (S_i + (N_i' \oplus v)) \oplus ((N_i \oplus g_i) - S_i) \quad (3)$$
$$P_{3i} = ((S_i \oplus v) - (P_{1i} \oplus TID_i' \oplus N_i)) \oplus ((P_{2i} \oplus TID_i \oplus N_i') - (S_i \oplus v)) \quad (4)$$

Equations in successful session Ses_{i+1}

$$K_i^1 = (TID_i - g_i^1) \oplus ((v^1 \oplus g_i^1) - N_i) \quad (5)$$
$$P_{1i}^1 = (S_i + (TID_i' \oplus g_i^1)) \oplus ((TID_i \oplus v^1) - S_i) \quad (6)$$
$$P_{2i}^1 = (S_i + (N_i' \oplus v^1)) \oplus ((N_i \oplus g_i^1) - S_i) \quad (7)$$
$$P_{3i}^1 = ((S_i \oplus v^1) - (P_{1i}^1 \oplus TID_i' \oplus N_i)) \oplus ((P_{2i}^1 \oplus TID_i \oplus N_i') - (S_i \oplus v^1)) \quad (8)$$

Equations in successful session Ses_{i+2}

$$K_i^2 = (TID_i' - g_i^2) \oplus ((v^2 \oplus g_i^2) - N_i') \quad (9)$$
$$P_{1i}^2 = (S_i + (TID_i'' \oplus g_i^2)) \oplus ((TID_i' \oplus v^2) - S_i) \quad (10)$$
$$P_{2i}^2 = (S_i + (N_i'' \oplus v^2)) \oplus ((N_i' \oplus g_i^2) - S_i) \quad (11)$$
$$P_{3i}^2 = ((S_i \oplus v^2) - (P_{1i}^2 \oplus TID_i'' \oplus N_i')) \oplus ((P_{2i}^2 \oplus TID_i' \oplus N_i'') - (S_i \oplus v^2)) \quad (12)$$

Proof: A can intercept the information transmitted in multiple sessions and perform XOR operation over the corresponding equations of the intercepted information. Thus he can obtain secret information and mount various attacks. In order to verify whether this attack is present or not, we perform the experiment depicted in Algorithm 6. We prepared a list of equations $\mathcal{L}$which consists of the equations for the information transmitted in an unsuccessful session Ses_i, a successful session Ses_{i+1} and another successful session Ses_{i+2}. These sessions are three consecutive sessions. We select the sessions in such a way that any other session cannot provide any extra benefit. The algorithm takes the list $\mathcal{L}$as an input where each equation in the list has two components that are tied with XOR operation. For example, the equation for K_i consists of two components ($TID_i - g_i$) and (($v \oplus g_i$) − Ni) that are tied with XOR operation. If it finds any pair of equations which has a common component tied by XOR operation, it applies XOR operation over these two equations and outputs a new equation which is added to $\mathcal{L}$. It selects this pair to apply the XOR operation because the XOR operation will suppress the common component and hence the resultant equation may become vulnerable. However, if any pair does not have any common component, the XOR operation cannot help. The XOR operation will increase the components in the resultant equation and this cannot be benefited to A. Thus it continues till it obtains a new equation in $\mathcal{L}$. According to our experiment, there is no new equation produced by the Algorithm 6. Therefore the proposed scheme is secure.

XOR-approximation: Approximate a given equation $A = (B + C) \oplus (D - E)$ into another equation $A' = (B \oplus C) \oplus (D \oplus E)$. The probability that $A = A'$ is $(0.75)^{d-1}$, where d is the length (bit size) of A, A', B, C, D, E[3].

Theorem 3: *The proposed object authentication scheme is secure from the attacks in the threat model under the XOR-approximation assumption.*

Proof: The equations used in the proposed scheme consist of +/- operation and A can convert these equations using XOR approximation and then try to mount the attacks mentioned in the threat model. However, the success probability depends on the successful approximation. The probability of successful approximation is $(0.75)^{d-1}$, where d is the length (bit size) of each secure information. Table 2 shows this probability on various values of d. Clearly, the probability decreases with increase in d. However, a large d value is computationally infeasible. Therefore, an appropriate value of d needs to be chosen which can be computationally feasible and the success probability to mount various attacks is sufficiently small.

[3] Replace +/- operation in $A = (B + C) \oplus (D - E)$ with XOR operation to obtain a new equation $A' = (B \oplus C) \oplus (D \oplus E)$. The LSB of A' is same as LSB of A since there is no carry or borrow input bit in LSB. However there can be carry/borrow input bit in other bits and maximum probability that i^{th} bit of A is equals to the i^{th} bit of A' is 0.75 [13]. Therefore, the probability of $A = A'$ is $(0.75)^{d-1}$, (d is the bit size of A and A').

Table 2: Success probability on various d values

d	1	2	32	64	96	128
β	1	7.5×2^{-3}	1.339366×2^{-13}	1.345425×2^{-27}	1.351512×2^{-40}	1.357627×2^{-53}

Security Comparison: We Compare The Proposed Scheme With A Selected Set Of Existing Authentication Schemes. Table 3 Shows That The Proposed Scheme Satisfies All The Security Requirements Mentioned In The Threat Model Except The Impersonation Attack. However, The Use Of Multiple Number Of Tags In Each Object Helps To Increase The Difficulty For The Adversary To Mount This Attack. The Existing Schemes Are Unable To Prevent Two Or More Attacks.

Table 3: Security assurance

	a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*
Weis et al.[2]	N	Y	N	N	N	Y	Y	Y	N
Randomized hash[2]	N	Y	Y	Y	Y	Y	Y	Y	N
Song et al.[3]	Y	Y	Y	Y	Y	N	Y	Y	N
Hyung-Joo et al.[9]	Y	Y	N	Y	Y	Y	Y	Y	N
Guo-Rui Li et al. [8]	Y	N	Y	Y	Y	N	N	N	N
Dhal et al.[11]	Y	Y	Y	Y	N	Y	Y	N	P
Proposed scheme	Y	Y	Y	Y	Y	Y	Y	Y	P

a: Eavesdropping, *b*: Man-in-the-middle attack, *c*: Replay attack, *d*:Traceability, *e*: Traceability between two successful sessions, *f*: Forward security, *g*: Backward security, *h*: De-synchronization attack, *i*: Impersonation attack, Y : Satisfy, N: Not satisfy, P: Partially satisfy.

B. Computational Overhead

We analyze the computational overhead of the proposed scheme and compare the scheme with the existing schemes. Table 4 illustrates the computation requirements in various schemes. In our analysis, we consider the operations used in the proposed scheme such as XOR, addition, subtraction, random number generation, and the other operations used in the existing schemes such as hash functions, attachment/detachment operation, etc. Table 4 shows that the tag in the proposed scheme uses most number of XOR and addition, subtraction operation. However, these are elementary operations. It uses only one heavyweight operation, i.e. random number generation. However, the tags in the existing schemes [3][8][9] use many heavyweight operations. The schemes proposed in [2] use minimum operations. However, these schemes are unable to prevent most of the attacks. Similarly the backend server uses many elementary operations in the proposed scheme whereas in the existing schemes [3][8][9], it uses many heavyweight operations. The reader in the proposed scheme uses no operation in the proposed scheme whereas the schemes proposed in [3][8][9][11] use one or more heavyweight operations. Therefore, the proposed scheme is lightweight in respect to the computation overhead in tag and can be deployable in real life environment.

C. Communication Overhead

Table 4: Number of operations performed in various scheme

	Tag					Reader					Backend Server				
	a	*b*	*c*	*d*	*e*	*a*	*b*	*c*	*d*	*e*	*a*	*b*	*c*	*d*	*e*
Weis et al.[2]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Randomized hash[2]	0	0	1	1	1	0	0	1	1	0	0	0	0	0	0
Song et al.[3]	6	0	6	3	1	0	0	0	0	1	$4n + 4$	0	6	2n + 1	0
Hyung-Joo et al.[9]	7	1	5	0	5	0	0	2	0	1	$4n + 4$	n	$n + 7$	0	$2n + 2$
Guo-Rui Li et al. [8]	2	0	7	5	1	0	0	0	0	1	$n + 1$	0	$4n + 3$	4n + 2	1
Dhal et al.[11]	$4m + 3$	2	0	0	0	0	0	0	1	1	$mn + 6m$	$2nm$	0	1	$2m + 1$
Proposed scheme	14	8	0	0	1	0	0	0	0	0	$4n^2m + 13m$	$6n^2m + 6m$	0	0	$2m + 1$

We compute the overhead due to communication between the components mentioned in the communication model.

Table 5: Communication overhead of various scheme

	Tag	Reader	Backend server
Weis et al.[2]	4	6	2
Randomized hash[2]	4	6	2
Song et al.[3]	4	9	5
Hyung-Joo et al.[9]	5	9	4
Guo-Rui Li et al. [8]	6	$5 + 6n$	$3n + 2$
Dhal et al.[11]	$3m + 4$	$6 + 6m + 2mn$	$3m + 4$
Proposed scheme	$4m + 4$	$8m + 6mn + 2$	$4m + 3nm + 1$

n: Number of objects, *m*: Number of tags attached to an object

Table 5 shows that the communication requirements for the existing schemes [2] [3][8][9] are less. However, the proposed scheme and the scheme in [11] require communicating more information due to the fact that multiple number of tags are present in each object. However, multi-tag arrangement helps to increase the difficulty for the adversary to mount attacks.

D. Storage Requirement

RFID tags have limited storage capacity. Therefore, we analyze the existing schemes and the proposed scheme in terms of storage requirements. Table 6 illustrates this analysis and it shows that the scheme proposed in this paper require storing 4 parameters. If we consider the maximum size of each parameter as 128 bits then the tag requires storing only 512 bits information. The tags in the existing schemes also require storing almost equal number of information bits. Though the backend server does not suffer from storage limitations, we analyze the storage requirement for these components as well. According to Table 6, the proposed scheme and the scheme in [11] require higher storage overhead in backend server. This is again due to the fact that each object is attached with multiple number of tags.

Table 6: Storage requirement

	Tag	Reader	Backend server
Weis et al.[2]	3	0	$3n$
Randomized hash[2]	1	0	n
Song et al.[3]	1	0	5
Hyung-Joo et al.[9]	2	0	$2n$
Guo-Rui Li et al. [8]	3	0	$5n$
Dhal et al.[11]	5	0	$4mn$
Proposed scheme	4	0	$8mn + n$

n: Number of objects, *m*: Number of tags attached to an object

V. CONCLUSION

Authentication is a necessary task in RFID technology due to its pervasiveness. Existing authentication schemes assume the objects are attached with single tag. However use of multiple number of tags to an object can enhance the detection probability of the object. Our work has motivated from the multi-tag concept which uses multiple number of tags for each object to increase the difficulty for the adversary to mount various attacks. The proposed authentication scheme is lightweight and secure which is verified through proper analysis. However, due to the responses from multiple number of tags for each object, the traffic congestion between reader and object is high. Also a suitable Physical Unclonable function (PUF) can be used to prevent the impersonation attack which is missing in the proposed scheme.

REFERENCE

[1] H. Chien, "Tree-Based Matched RFID Yoking Making It More Practical and Efficient", Journal of Computer Network and Information Security, vol. 1, no. 1, pp. 1-9, 2009.

[2] V. K. N. Kumar and B. Srinivasan, "Design and Development of Biometrics Secure Person Detection System for E-Passport using Cryptographic Security Protocols", Journal of Computer Network and Information Security, vol. 5, no. 12, pp. 80-90, 2013.

[3] L. Bolotnyy and G. Robins, "Multi-Tag RFID Systems," Journal of Internet Protocol Technology (IJIPT), Special issue on RFID: Technologies, Applications, and Trends, vol. 2, no. 3/4, pp. 218−231, 2007.

[4] S. Dhal and I. Sen gupta, "Managing Authentication and Detection Probability in Multi-tag RFID System", Journal of Information Assurance and Security, vol. 9, no. 6, pp. 316-328, 2014.

[5] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," in Proceedings of the 1st Conference on Security in Pervasive Computing, pp. 201−212, 2004.

[6] B. Song and C. J. Mitchell, "RFID Authentication Protocol for Low-cost Tags," in Proceedings of the 1st ACM Conference on Wireless Network Security, pp. 140−147, 2008.

[7] C. C. Tan, B. Sheng, and Q. Li, "Serverless Search and Authentication Protocols for RFID," in Proceedings of the 5th Conference on Pervasive Computing and Communication, pp. 3−12, 2007.

[8] G. Tsudik, "A family of dunces: Trivial RFID identification and authentication protocols," in

Proceedings of Privacy Enhancing Technologies Symposium, pp. 45−61, 2007.
[9] M. Burmester, T. V. Le, and B. D. Medeiros, "Provably secure ubiquitous systems: Universally composable RFID authentication protocols," in Proceedings of SECURECOMM, pp. 1−9, 2006.
[10] M. Conti, R. D. Pietro, and L. V. Mancini, "RIPP-FS: an RFID Identification, Privacy Preserving Protocol with Forward Secrecy," in Proceedings of the 5th Conference on Pervasive Computing and Communication, pp. 229−234, 2007.
[11] G. R. Li, Y.Wang, C. R.Wang, and J. S. He, "Emap: An efficient mutual authentication protocol for passive RFID tags," Journal of Automation and Computing, vol. 9, pp. 108−112, 2012.
[12] H. J. Kim and M. S. Jun, "Light-weight Mutual Authentication RFD Protocol for Multi-Tags conforming to ESC Class-1 Generation-2 Standards," in Proceedings of the 5th International Conference on Computer Sciences and Convergence Information Technology, pp. 34−39, 2010.
[13] P. Rizomiliotis, E. Rekleitis, and S. Gritzalis, "Security Analysis of the Song-Mitchell Authentication Protocol for Low-cost RFID Tags," Communications Letters, vol. 13, no. 4, pp. 274−276, 2009.
[14] S. Dhal and I. Sengupta, "A New authentication Protocol for Multi-tag RFID Applicable to Passive Tag," in Proceedings of the International Conference on Communication, Computing & Security, pp. 880−888, 2012.
[15] C. E. Shannon, "A Mathematical Theory of Communication," The Bell System Technical Journal, vol. 27, pp. 379−423, 1984.
[16] D. Mukhopadhyay, "Design and Analysis of Cellular Automata Based Cryptographic Algorithms," Ph. D thesis, Indian Institute of Technology Kharagpur, India, 2007.

Authors' Profiles

Subhasish Dhal a B.Sc(H) degree in Computer Science from Vidyasagar University, Midnapore in 2002, and a MCA degree from NIT Durgapur in 2005. He also has received an M. tech degree in Computer Sc. and Engineering from NIT Rourkela in 2009. From August 2005 till August 2007 he worked in Asutosh College, Kolkata as a lecturer and from August 2009 till December 2009 he worked in IE & IT, Durgapur as a lecturer. Since December 2009, he has been a research scholar in the department of Computer Science & Engineering in IIT Kharagpur. His research interests are in the areas of Security in RFID, Mobile Networks and Key Management and Distribution.

Indranil Sen Gupta is a professor of Department of Computer Science & Engg. in the Indian Institute of Technology, Kharagpur (India). He received his Bachelor's, Master's and Doctorate degrees in Computer Science from University of Calcutta, India. His research interests are primarily in the field of Information Assurance, Cryptography & Network Security, Testing & fault diagnosis and CAD for VLSI. He has published more than 90 research articles in leading journals, conference proceedings and books including ACM Transactions, IEEE, JCC and JSA. He serves in editorial boards of several International Journals and has served in program committees of several international conferences. He has two decades of rich experience in teaching and research.

How to cite this paper: Subhasish Dhal, Indranil Sen Gupta,"Object Authentication Using RFID Technology: A Multi-tag Approach", IJCNIS, vol.7, no.4, pp.44-53, 2015.DOI: 10.5815/ijcnis.2015.04.06