International Journal on Semantic Web and Information Systems
Volume 16 • Issue 3 • July-September 2020

Secure Timestamp-Based Mutual Authentication Protocol for IoT Devices Using RFID Tags

Aakanksha Tewari, National Institute of Technology, Kurukshetra, India
Brij B. Gupta, National Institute of Technology, Kurukshetra, India

ABSTRACT

Internet of Things (IoT) is playing more and more important roles in our daily lives in the last decade. It can be a part of traditional machine or equipment to daily household objects as well as wireless sensor networks and devices. IoT has a huge potential which is still to be unleashed. However, as the foundation of IoT is the Internet and all the data collected by these devices is over the Internet, these devices also face threats to security and privacy. At the physical or sensor layer of IoT devices the most commonly used technology is RFID. Thus, securing the RFID tag by cryptographic mechanisms can secure our data at the device as well as during communication. This article first discusses the flaws of our previous ultra-lightweight protocol due to its vulnerability to passive secret disclosure attack. Then, the authors propose a new protocol to overcome the shortcomings of our previous work. The proposed scheme uses timestamps in addition to bitwise operation to provide security against de-synchronization and disclosure. This research also presents a security and performance analysis of our approach and its comparison with other existing schemes.

KEYWORDS

Anonymity, Authentication, Confidentiality, Internet of Things, RFID tags

1. INTRODUCTION

While Internet is being referred as a framework allowing people to gather and store information or communicate with each other across the globe; the Internet of things is gradually unfolding allowing daily objects to be able communicate and collect data and be a part of the web (Ashton, 2009). IoT is growing at an unprecedented rate including wide range of applications such as weather monitoring, farming, disaster management, healthcare and smart homes and security, etc. (Fuqaha et al. 2015). IoT networks are highly dynamic distributed networks promoting Information and communication technology domain made up of a large number of devices and sensors sending and receiving a lot of information all the time. There is no doubt that IoT will play remarkable role in improving the quality our lives (Grabovica et al. 2016).

IoT empowers physical objects to be able think and hear or even see their surroundings in order to perform the tasks they are allotted and make decisions by sharing information with other objects (Atzori et al. 2010). The objects which were once conventional in their working are now in transition to be smart objects by getting assistance from new areas like pervasive computing, wireless sensor networks, cloud computing (Li et al., 2018; Li et al., 2015; Shen et al., 2018), Radio frequency identification, etc. (Sicari et al., 2015).

DOI: 10.4018/IJSWIS.2020070102

Although in order to perceive maximum potential of IoT the technologies that enable IoT also needs to grow at an equal proportion to match the requirements of the industry and people as the devices are required to be competent to the customer's use (Mukherjee, 2015).-In this paper, our goal is to address those issues and assess where IoT stands today and what will be the future aspects of this domain (Kashif et al., 2016; Fan et al., 2017).

The IoT devices have limited resources and require updating and identification of other objects as well as server (Gupta et al., 2016; Stergiou, Psannis et al., 2018). Mutual authentication using RFID tag is the most common way to secure the devices from intrusion and ensure data integrity and confidentiality. But due to the limited computation and storage capabilities we need some lightweight mechanisms for this purpose (Zhuang et al., 2018; Gao et al, 2018; Lin, Yan et al., 2018).

RFID is a very promising enabling technology for the IoT paradigm as it provides resistance from heat and magnetic waves and more storage space as compared to other technologies. It also ensures even at long distances at lower costs (Zhuang et al., 2018). However, due to the insecure communication channel between the reader and the tag we need to ensure secure message exchange by using some authentication or identification protocols. To ensure security with lower complexity various schemes have been proposed (Fan et al., 2017; Li et al., 2018). However, a number of attacks have also been formulated e.g., eavesdropping, replay and desynchronization attacks. By carrying out such attacks adversary can gather information from the tag and later on it can be used to adversary's benefit and can even lead to tag corruption, full disclosure of information or impersonation (Akgun et al., 2014).

Authentication protocols using RFID tags are classified into four types (Chien, 2007); first is full-fledged class of protocols which consists of protocols which use classical cryptographic encryption and decryption protocols and have large computational overhead, The second class comprises of simpler protocols which require techniques such as elliptic curve cryptography, random number generator and hash function, etc., for mutual authentication purpose. The third class consists of lightweight mutual authentication protocols which use comparatively simple functions like random number generators, checksums etc. The fourth class of protocols is the ultra-lightweight protocols which only use bitwise operations such as OR, AND, XOR, Rotation or permutation, etc., these have the lowest overhead in terms of storage and computation.

2. OUR CONTRIBUTION

In this paper, we propose a new mutual authentication scheme which addresses the issues in our previous work. The primary objectives behind this work are:

- To perform a study of flaws in our previous work and the reasons that can lead to any more attacks.
- Use of bitwise operations makes protocols easier to implement but also due to the simplicity they may be easy to crack. Therefore, we have introduced the concept of timestamps and Pseudo-Random number generators.
- The use of timestamps makes our protocol timebound, thus the communicating parties will know if there is any delay due to interception.
- Use of PRNGs makes the data in communication random and independent from previous sessions.

The rest of the paper is organized as follows: In the next section we discuss the background of IoT security, along with some recent RFID authentication techniques. In the section three we discuss our proposed solution. Section 5 presents a detailed security analysis of our proposed solution. In the section 6 we present a performance analysis of our protocol followed by section 7 where we conclude our paper and discuss some future directions.

3. RELATED WORK

The security protocols serve the purpose of authentication in order to ensure device privacy and information security. Due to weak security RFID tags can be vulnerable to threats posed by a 3rd party which can result into loss of critical information or even tag corruption. Thus, strong cryptographic mechanisms are required in order to secure and privacy is major concern for IoT devices.

SLAP (Zhuang et al., 2018), a recent addition to the class of ultra-lightweight protocols also utilizes only bitwise operations like rotation and exclusive-OR. KMAP (Mujahid et al. 2017), another lightweight mutual authentication scheme which also uses rotation and XOR operations in addition to random number generator and a counter. Some other approaches SASI+ (Khokar et al., 2016), RCIA (Khokar et al., 2015), R2AP (Zhuang et al., 2014) have also been proposed which fall under the same category.

Although, the above protocols have claimed to be secure against most security threats; Safkhani and Bagheri (2018) have proved that the above protocol are vulnerable to desynchronization attacks. According to Safkhani and Bagheri (2018), the above-mentioned schemes can be mapped to a generalized version of ultra-lightweight protocol (GUMAP). Further, they carried out a desynchronization attack on GUMAP which showed that SLAP, KMAP, SASI+ and RCIA are all vulnerable.

Tsudik (2006) proposed YA-TRAP which is a timestamp based mutual authentication protocol in order to ensure security against tag tracing. They also proposed an updated version of above protocol (Tsudik, 2006) which was later found to be vulnerable to replay attacks.

Okhubo et al. (2003) proposed a hash-based technique which used randomized hash lock and XOR based OTP but this scheme had high cost of tag search at back end server. Weis et al. (2004) proposed another hash lock technique as an improvement of (Okhubo et al., 2003) as it handled the searching at the back-end server efficiently. This approach used a Meta Id which obtained applying hash on a random number. Juels and Weis (2005) proposed a protocol based on parity concept and symmetric key authentication but it was vulnerable to noise affecting the parity values.

Some other protocols which used classical mechanisms were also proposed for RFID authentication. Feldhofer et al. (2004) proposed a two-way mutual authentication protocol using symmetric cipher (AES) but this protocol has high overhead due to key management and heavy computations and power consumption. The concept of ECC-based mutual authentication protocols was introduced by Wolkesfoster (2005). Tulys and Batina (2006) proposed first ECC-based authentication approach using Schnorr's identity protocol (1989). They proposed another scheme (Batina et al., 2007) using Okamoto's ID protocol (1992). Lee et al. (2008) however, showed that these schemes cannot ensure anonymity (Table 1 shows comparison of some existing ECC based protocols).

Other protocols have used lightweight version of HB (Hopper & Blum, 2001). The first HB protocol for RFID was proposed by Weis et al. followed by HB+ which were analyzed by Katz and Shin (2006a, 2006b) they showed that these protocols are secure against active attacks during parallel executions. These protocols are considered secure as they are based on learning parity with noise (LPN) problem, which assumed to be hard over random instances. However, these protocols are vulnerable to man-in-the middle attacks.

Another category of solutions is the use of pseudo ID (or a pseudonym) where tags have random IDs which are updated after every session; thus, the tag's original ID remains secure. However, these protocols are vulnerable to tracking, eavesdropping as well as de-synchronization attacks. Some protocols use only bitwise operations in order to reduce the complexity in terms of computation at RFID tags. Lopez et al., (2006a; 2006b; 2006c) proposed a family of ultra-lightweight protocols: LMAP, M2AP and EMAP. But these protocols suffer from full-disclosure and de-synchronization attack (Table 2 shows comparison of some existing ultra-lightweight protocols).

Table 1. Comparative analysis of some ECC-based authentication protocols

	Tag's Communication Cost	Anonymity	Forward secrecy	Mutual Authentication
Chen et al. (2011)	231	Yes	Yes	No
Liao et al. (2013)	210	Yes	Yes	No
Lee et al. (2010a)	189	Yes	Yes	No
Lee et al. (2010b)	189	Yes	Yes	No
Farash (2014)	186	Yes	Yes	Yes
Batina et al. (2012)	168	Yes	Yes	No

4. PROPOSED SOLUTION

In section we first briefly discuss our previous protocol (Tewari and Gupta, 2016) followed by a brief discussion of disclosure attacks as shown by Safkhani and Bagheri (2016). We then present a new approach using timestamps and Pseudo random number generator (only at the back-end server's side) to address eavesdropping and disclosure attacks.

4.1. Our Previous Protocol

In (Tewari and Gupta, 2016) we proposed an ultra-lightweight protocol for mutual authentication between the reader and the tag. The protocol involves the following entities: the tag, the reader and the backend database server. Our protocol uses only bitwise operations, i.e., bitwise XOR and rotation operations. The random number generation is performed by the server, so it does not affect the performance of our protocol. Since, the resources and computational capabilities of the IoT devices is limited we proposed an ultra-lightweight mutual authentication protocol, the steps followed by our protocol are given below (Figure 1 shows a flow diagram of the protocol):

1. The protocol session is initialized by the reader, as it sends a "*hello*" message to the tag
2. When the tag receives the message, it sends its old as well as new values of pseudo ID values as $<IDS_{new}, IDS_{old}>$ to the reader.
3. On receiving tag's response, the IDS values are searched for a match at the back-end server. If no match is found, then the session is dropped. In case matching values are found, then two cases arise:

Table 2. Comparative analysis of some ultra-lightweight authentication protocols

	Tag's Storage Cost	Tag's Communication Cost	Tracking	Mutual Authentication
LMAP	576	384	No	Yes
M2AP	576	480	No	Yes
EMAP	576	480	No	Yes
Our Previous Protocol (Tewari and Gupta, 2016)	672	288	No	Yes

Case I: both IDS values sent by the tag match the values at the back-end server. Therefore, we set:

$(IDS_{old})_{server} = (IDS_{new})_{server}$;
$(K_{old})_{server} = (K_{new})_{server}$;
Case II: $(IDS_{old})_{tag} = (IDS_{new})_{server}$, (last session was unsucessful). Therefore, we set:
$(IDS_{new})_{server} = (IDS_{old})_{server} = (IDS_{new})_{tag}$;
$(K_{new})_{server} = (K_{old})_{server} = tag's\ (K_{new})_{tag}$;

After doing this check, IDS_{new} *and* K_{new} are used for all the further computations and are referred as *IDS* and *K*.

4. The PRNG generates two 96-bit random numbers m and n. Then, it calculates:

$P = IDS \oplus m \oplus n$;
$Q = K \oplus n$;
$R = Rot(Rot(K \oplus n, IDS), K \oplus m)$;

5. The values <*P,Q, R*> are sent to the device tag.
6. On receiving the<*P,Q, R*>, the tag performs the following computations:

- Calculate:$n = Q \oplus K$;
- and,$m = P \oplus n \oplus IDS$;
- Then, calculate:$R' = Rot(Rot(K \oplus n, IDS), K \oplus m)$;
- If $R' \neq R$,
  - then abort session
- Else,
  - Calculate: $S = Rot(Rot\ (IDS \oplus m, K), R' \oplus n)$;

7. <*S*> is sent to the reader.
8. On receiving<*S*>, thereader performs the following computations:

- Calculate:$S' = Rot(Rot\ (IDS \oplus m, K), R \oplus n)$;
- If $S' = S$,
  - Then, mutual authentication process is successful.
- Else,
  - abort session

After a successful authentication session, the updation of K and IDS is done as follows:

$IDS_{old} = IDS_{new}$; $K_{old} = K_{new}$;
$IDS_{new} = Rot(IDS \oplus n, K \oplus n), IDS \oplus m)$;
$K_{new} = Rot(R \oplus n, IDS \oplus m)$;

4.2. Secret Disclosure Attack Against our Protocol

Safkhani and Bagheri (2016) proved that our protocol is vulnerable to passive disclosure attacks, as follows:

Learning Phase: here the adversary eavesdrops over a single session of the protocol and saves the messages and the values: IDS_{old}, IDS_{new}, *P, Q, R* and *S*.

Passive Secret Disclosure Attack: Here, the adversary uses the values stored to obtain all the secret values of the tag as follows in Figure 2:

Thus, using the above algorithm the adversary is able to disclose all the secret data of the tag by eavesdropping over one session.

4.3. Our Proposed STMAP Protocol

In this section we propose a new mutual authentication protocol for IoT devices that ensures secure the communication by using timestamps and PRNGs. We have assumed that the channel between the

Figure 1. Flow diagram our previous approach

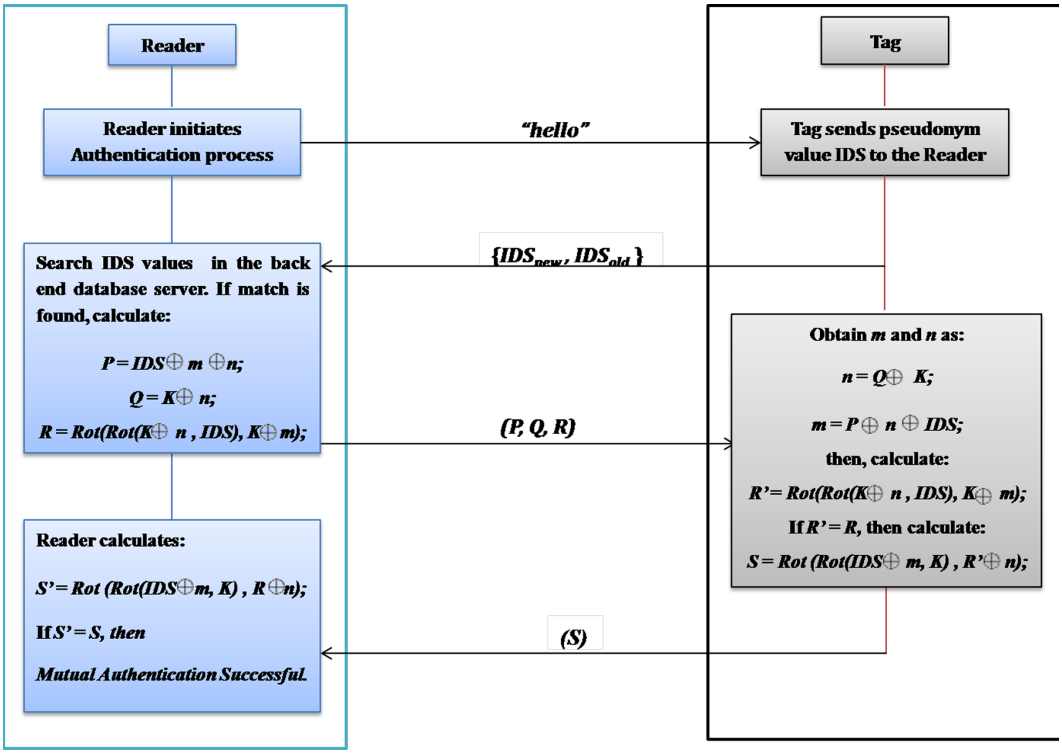


Figure 2. De-synchronization attacks algorithm

for i = 0, ..., L, the adversary does:

$S \gg i \rightarrow x;$
$IDS \oplus x \rightarrow m;$
$P \oplus m \oplus IDS \rightarrow n;$
$Q \oplus n \rightarrow K;$

If $Rot(Rot(K \oplus n, IDS), K \oplus m) = R$:

$IDS \rightarrow IDS_{old}$
$K \rightarrow K_{old}$
$Rot(Rot(IDS \oplus n, K \oplus n), IDS \oplus m) \rightarrow IDS_{new};$
$Rot(R \oplus n, IDS \oplus m) \rightarrow K_{new};$
returns IDS_{old}, IDS_{new}, K_{old}, K_{new}, *n and m.*

reader and the server is secure. This protocol is executed in three phases which are discussed next (Figure 3 below shows the list and description of parameters and operators used).

Figure 3. Preliminaries

IDS: pseudo-Identifier updated after successful authentication
K: session key updated after every session
T_i : i^{th} Timestamp
A: authentication parameter sent by Tag
X: Authentication Parameter sent by Reader
r_i : Random numbers generated by the PRNG
R_i : Variables to mask the random variables
η : Maximum transmission delay
PRNG(N,x): pseudo-random sequence generated by *generator* with input or seed *(N, x)*.
$\oplus$: bitwise XOR operation
Rot(X,Y): rotates *X* left by *wt(Y)* (mod 96) bits

4.3.1. Pre-registration Phase

- For each tag the back-end server stores two pseudonym *ID* values. One is from the previous session which is IDS_{old} and another is to be used in the new session which is denoted as IDS_{new}.
- For each is session there is one key *K* which is updated after the session ends.
- The tag stores only one *IDS* value unlike our previous protocol (where tag had both IDS_{new} and IDS_{old}) which is updated after every session depending upon the following cases:
  - Case I: $IDS_{(at\ Tag)} = IDS_{new(at\ Server)}$ and $K = K_{new(at\ Server)}$; which means that the last authentication session was successful.
  - Case II: $IDS_{(at\ Tag)} = IDS_{old(at\ Server)}$ and $K = K_{new(at\ Server)}$; which means that the previous session was unsuccessful where server successfully authenticated the tag but tag couldn't.
  - Case III: $IDS_{(at\ Tag)} = IDS_{old(at\ Server)}$ but $K \neq K_{new(at\ Server)}$; this means that the tag is corrupted and the in this case the server immediately aborts the session.
- We have also used timestamps to check for any MITM or forgery attacks etc. We have defined a threshold 'η' which is maximum transmission delay and time difference between the transmission $\Delta T = T_i - T_j$ should not exceed the value 'η'.

4.3.2. Initialization Phase

The reader initiates the session by sending a '*hello*' message to the tag.

4.3.3. Registration Phase

- On receiving the readers' request the tag calculates: $A = (K \oplus IDS \oplus T_1)$ and sends $<IDS, A>$ to the server.
- On receiving the tag's response, the server first calculates $T_1 = A \oplus K \oplus IDS$, using the *K* value stored in its memory for the corresponding *IDS* value. If the reader is successful in finding the correct *K* the correct value of T_1 will be computed. The next step is to calculate: $\Delta T = T_2 - T_1$. If $\Delta T \leq \eta$ then the tag is considered to be legitimate or uncorrupted. (as shown in Figure 4.)

- The reader now calculates the authentication parameter *X* as follows in Figure 5:
- Then, the new random numbers (r_1, r_2, r_3, r_4) are also encrypted as:

$R_1 = r_1 \oplus T_2 \oplus K;$
$R_2 = r_2 \oplus R_1;$
$R_3 = r_3 \oplus r_2 \oplus K;$
$R_4 = R_3 \oplus R_2 \oplus r_4;$

Figure 4. Tag's authentication by the Reader

```
Input: <IDS, A>
Retreive K from the back end server using IDS value
If (No Match Found)
Then, Corrupted Tag
        Abort session
Else,
T1→ A ⊕K⊕ IDS
ΔT→  T2 – T1
If (ΔT ≤ η)
Legitimate Tag
   Else
      Corrupted Tag
     Abort Session
```

Figure 5. Calculation of Reader's authentication parameter algorithm

```
X→ IDS
for(I→ 1 to 4 )
      ri = PRNG()
      X = Rot((X ⊕ ri) , Ki)
      Ki+1 = (Ki + 1) mod 96
```

- Then, the reader sends $<X, R_1, R_2, R_3, R_4, T_2>$ to the tag for the next step.
- The tag on receiving the response $<X, R_1, R_2, R_3, R_4, T_2>$ the tag first checks the timestamps if: $\Delta T = T_2 - T_1 \leq \eta$, then it retrieves the random numbers as:

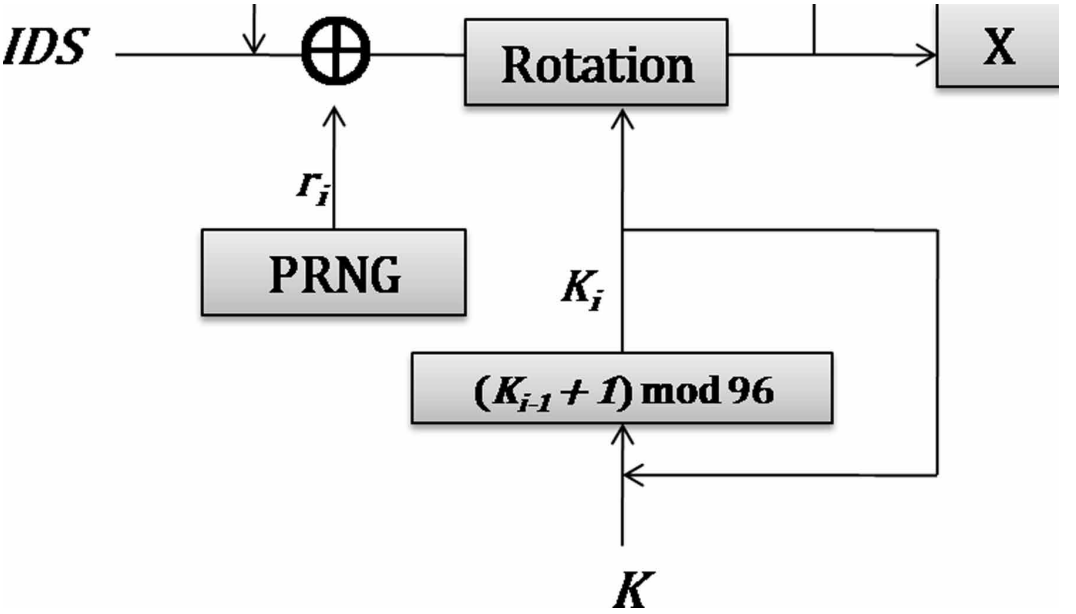
$r_1 = R_1 \oplus T_2 \oplus K$
$r_2 = R_2 \oplus R_1$
$r_3 = R_3 \oplus r_2 \oplus K$
$r_4 = R_3 \oplus R_2 \oplus R_4$

And using these values the tag calculates X' as shown in Figure 6. If $X' = X$ then, the authentication is successful and session ends.

4.3.4. IDS and Key Updation

- At the end of the session if server has successfully authenticated the reader, then it updates its *IDS* and *K* values as:

Figure 6. Calculation of Reader's authentication parameter block diagram



$IDS_{old} = IDS_{new}$
$IDS_{new} = Rot(IDS \oplus K, r_1)$
$K_{new} = Rot(K \oplus r_1, r_2);$

- At the tag's side the values are updated as:

If the tag receives the readers' message in time then: $IDS_{new} = Rot(IDS \oplus K, r_1)$ and $K_{new} = Rot(K \oplus r_1, r_2)$;Else if $\Delta T = T_2 - T_1 \geq \eta$, then the message is assumed to be forged and the session is immediately aborted without updating any values. Else, if the tag does not receive any response back from the reader until the session expires, it means that the message might have been dropped somehow, but the reader may have updated its *IDS* and *K* values. Thus, the tag only updates it's *K* value as: $K_{new} = Rot(K \oplus r_1, r_2)$; So, in the next session the server knows that the last session was unsuccessful (as shown in Figure 7).

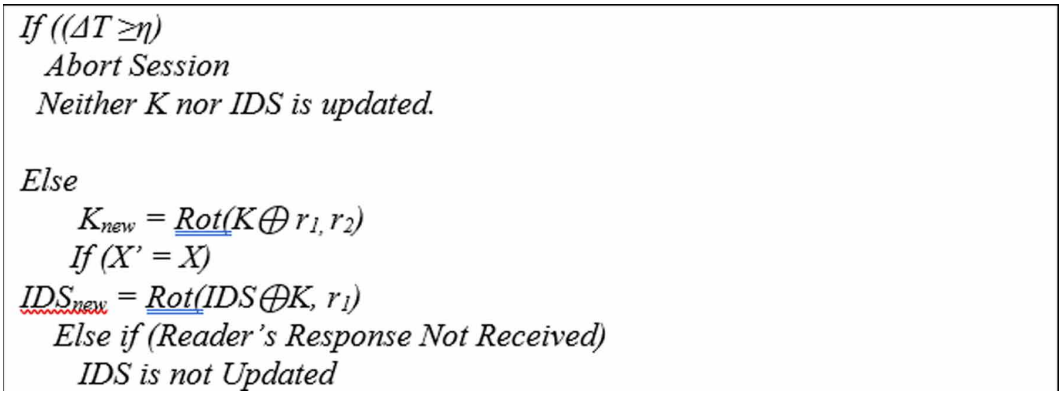
5. SECURITY ANALYSIS

In this section, we will show the strength of our protocol against various attacks. The basic system requirements that need to be fulfilled by an authentication protocol are anonymity, forward secrecy and confidentiality. In addition, our protocol provides security against the following attacks:

5.1. A1: Mutual Authentication

Our protocol two-way authentication i.e. server authenticates the tag and vice versa. The tag authenticated if $T_1 = A \oplus K \oplus IDS$ is correctly calculated so that $\Delta T = T_2 - T_1 \leq \eta$. Similarly, server/reader is successfully authenticated if $X' = X$ which is calculated using random numbers and timestamp.

Figure 7. Key and IDS Updation by the Tag



5.2. A2: Tracking

Our protocol has high resistance to tracking, the anonymity is increased as we are not sending any variable or data twice. The use of random variables also makes tracking difficult. All the variables in transit are temporary so each session a new set of variables is initialized. Even if the *IDS* value is not changed after the session the key *K* is still not known to the attacker (Figure 8).

5.3. A3: Forgery Attack

The protocol uses timestamps which are validated when receiver gets a message from the other party on basis of η whichis the maximum transmission delay. If the message is forged then the time difference between the timestamps will exceed the transmission delay $\Delta T = T_i - T_j$. Even if the value of timestamps is forged the authentication variables would be calculated incorrectly leading to session termination.

5.4. A4: Eavesdropping

Our protocol provides security against eavesdropping due to use of random numbers and temporary variables. As eavesdropping can happen anytime but its affect can be minimized as data collected can be useless after a certain time. The variables in transit *A, IDS, X,* R_1, etc., are changed after every session. So, there is no dependence between two sessions.

5.5. A5: Man-in-the-Middle

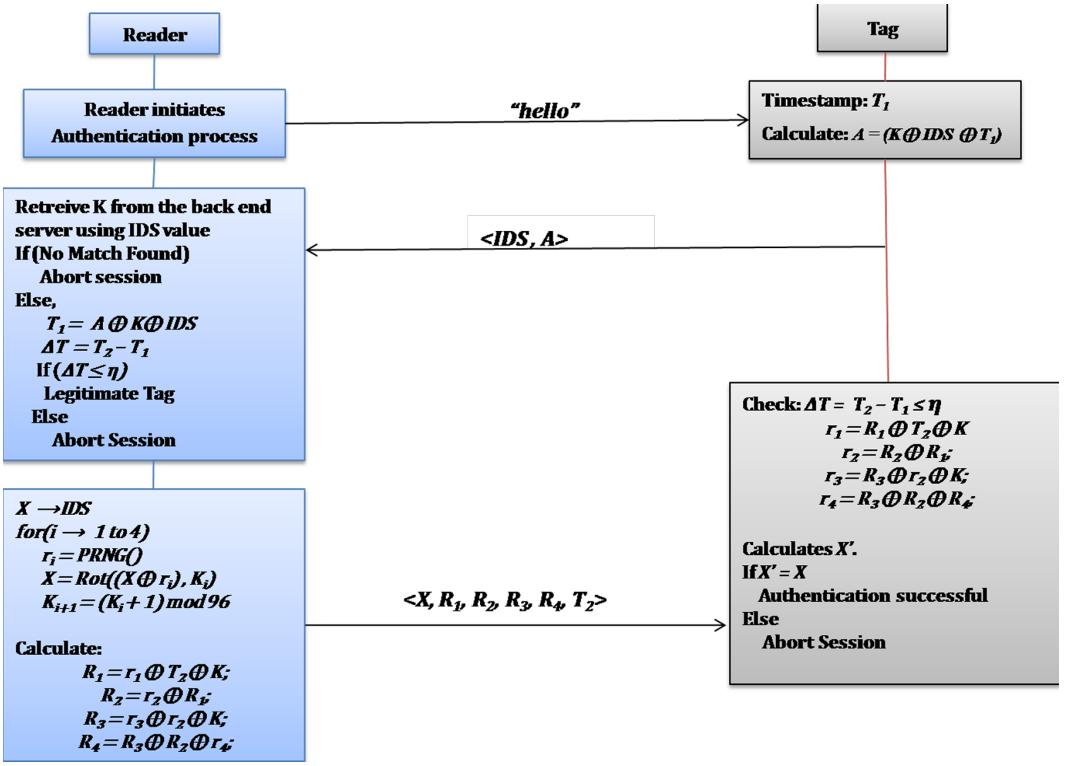
Our protocol provides security against MITM attacks in case if the messages are just replayed during another session, they cannot affect the tag or the server due to use new set parameters at every session. Even if the *IDS* is not changed after a session the key value is changed which is not available to the attacker.

5.6. A6: De-Synchronization Attacks

Our protocol provides security against De-synchronization attacks by introducing new cases for updation of *IDS* and *K*. Thus, the tag only has one value for IDS although the server keeps both IDS_{old} and IDS_{new}. These values updated after every session depending upon the following cases:

- Case I: $IDS_{(at\ Tag)} = IDS_{new(at\ Server)}$ and $K = K_{new(at\ Server)}$; which means that the last authentication session was successful.
- Case II: $IDS_{(at\ Tag)} = IDS_{old(at\ Server)}$ and $K = K_{new(at\ Server)}$; which means that the previous session was unsuccessful where server successfully authenticated the tag but tag couldn't.
- Case III: $IDS_{(at\ Tag)} = IDS_{old(at\ Server)}$ but $K \neq K_{new(at\ Server)}$; this means that the tag is corrupted and the in this case the server immediately aborts the session.

Figure 8. STMAP flow diagram



Thus, if any discrepancy is found in the IDS and K values it is immediately detected. Even if the attacker has IDS, the K value still remains a secret. The use of a set of random numbers for calculating X makes it hard to calculate it's correct value.

6. PERFORMANCE ANALYSIS

In this section we evaluate the performance of our proposed scheme on the basis of its computation, storage and communication cost for each device tag. As our approach only requires XOR (⊕) and left rotation (Rot(.,.)) thus it has very low computation cost.

Each tag requires to store three 96-bit values which are: *IDS, K* and device tag ID. Thus, the total storage requirements are 3*L* bits where $L = 96$(i.e., $3 \times 96 = 288$ bits). During the execution, the tag also stores (r_1, r_2, r_3, r_4) i.e., $L = 96$(i.e., $4 \times 96 = 384$ bits). Thus, the total storage during protocol session is:

Storage Cost = $7L = 7 \times 96 = 672$ bits

Tag's processing/computation time:

- During protocol run: 17 XOR operations (O(1)), 4 Rotations (O(N*(L-1)))
- Updation of (IDS, K): 2 XOR operations (O(1)), 2 Rotation (O(N*(L-1)))

7. CONCLUSION

In this paper, we presented a new ultra-lightweight mutual authentication protocol for IoT device tags which also uses timestamps. Our protocol also takes into account the vulnerability of our previous work and addresses with the use of timestamps which prevent any attempt of de-synchronization by the adversary. This protocol applies recurring rotation over the authentication parameter sent from reader to the tag so that the secret values cannot be extracted from it by eavesdropping. In addition, our protocol still has a very low computation and communication cost at the tag's side. The pseudo random number generator is used only at the back-end server once. The tag only performs bitwise operations to authenticate the reader and generate its own authentication parameter. Further our protocol is also secure from any vulnerability due to modular operations or use of addition or multiplication operations. (Table 3 shows a comparison of our approach with existing solutions.)

Table 3. Comparative analysis of our protocol with existing solutions

	Storage Cost	Communication Cost	Operation Used	De-synchronization Attacks	Disclosure Attacks	Forgery	Mutual Authentication
LMAP (Lopez et al., 2006a)	6L	4L	+, ⊕, OR	No	No	Yes	Yes
M2AP (Lopez et al., 2006b)	6L	5L	+, ⊕, AND, OR	No	No	Yes	Yes
EMAP (Lopez et al., 2006c)	6L	5L	⊕, AND, OR	No	No	Yes	Yes
SASI (Chien, 2007)	7L	4L	+, ⊕, AND, OR, Rot(A, B)	No	No	Yes	Yes
RAPP (Tian et al., 2012)	5L	2L	⊕, AND, OR, Rot(A, B), Per(A, B)	No	No	Yes	Yes
Gossamer (Lopez et al., 2006)	7L	5L	+, ⊕, AND, Rot(A, B), MixBits	No	Yes	Yes	Yes
FLMAP (Sadighian et al., 2006)	3L	4L	h(), PRNG, ⊕, OR, AND	No	No	Yes	Yes
LRTC (Dimitrou, 2005)	1L	-	h(), PRNG	No	Yes	No	No
Our Previous Protocol	7L	3L	⊕, Rot(A, B)	Yes	No	Yes	Yes
Our New Protocol	7L	2L	+, ⊕, Rot(A, B), Timestamp threshold check (-)	Yes	Yes	Yes	Yes

ACKNOWLEDGMENT

This research work is being funded by Department of Electronic and Information technology (DeitY), Ministry of Communications and IT, Government of India.

REFERENCES

Akgün, M., Uekae, T., & Caglayan, M. U. 2014. Vulnerabilities of RFID security protocol based on chaotic maps. In *Proceedings of the 2014 IEEE 22nd International Conference on Network Protocols* (pp 648–653). IEEE Press. doi:10.1109/ICNP.2014.103

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. *IEEE Communication Surveys & Tutorials, 17*(4).

Ashton, K. (2009). That "Internet of Things" thing. *RFiD Journal*.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. doi:10.1016/j.comnet.2010.05.010

Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., & Verbauwhede, I. (2007, March). Public-key cryptography for RFID-tags. In *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)* (pp. 217-222). IEEE.

Batina, L., Seys, S., & Singeee, D. (2012). Hierarchical ECC-based RFID authentication protocol. In *Proc. RFID Secur. Privacy* (pp. 183–201). Academic Press. doi:10.1007/978-3-642-25286-0_12

Chen, Y., Chou, J. S., Lin, C. F., & Wu, C. L. (2011). A Novel RFID Authentication Protocol based on Elliptic Curve Cryptosystem. *IACR Cryptology ePrint Archive*, 381.

Chien, H.-Y. (2007). SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. *IEEE Transactions on Dependable and Secure Computing*, *4*(4), 337–340. doi:10.1109/TDSC.2007.70226

Dimitriou, T. (2005, September). A lightweight RFID protocol to protect against traceability and cloning attacks. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks SecureComm 2005* (pp. 59-66). IEEE. doi:10.1109/SECURECOMM.2005.4

Fan, K., Ge, N., Gong, Y., Li, H., Su, R., & Yang, Y. (2017). An ultra-lightweight RFID authentication scheme for mobile commerce. *Peer-to-Peer Networking and Applications*, *10*(2), 368–376. doi:10.1007/s12083-016-0443-6

Farash, M. (2014). Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography. *The Journal of Supercomputing*, *70*(2), 987–1001. doi:10.1007/s11227-014-1272-0

Feldhofer, M., Dominikus, S., & Wolkerstorfer, J. 2004. Strong authentication for RFID systems using AES algorithm. In *Proceedings of Workshop on Cryptographic Hardware and Embedded Systems*. Academic Press. doi:10.1007/978-3-540-28632-5_26

Gao, C. Z., Cheng, Q., He, P., Susilo, W., & Li, J. (2018). Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack. *Information Sciences*, *444*, 72–88. doi:10.1016/j.ins.2018.02.058

Grabovica, M., Dražen Pezer, S. P., & Kneževiü, V. (2016). *Provided security measures of enabling technologies in Internet of Things (IOT): A survey*. IEEE. doi:10.1109/ZINC.2016.7513647

Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*. Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0105-3

Hopper, N. J., & Blum, M. (2001). Secure human identification protocols. In C. Boyd (Ed.), Advances in Cryptology - ASIACRYPT 2001 (pp. 52-66). Springer-Verlag. doi:10.1007/3-540-45682-1_4

Juels, A., & Weis, S. A. (2005, August). Authenticating pervasive devices with human protocols. In *Annual international cryptology conference* (pp. 293–308). Springer; . doi:10.1007/11535218_18

Katz, J., & Shin, J. S. (2006). Parallel and concurrent security of the HB and HB+ protocols. In S. Vaudenay (Ed.), EUROCRYPT (pp. 73-87). Springer.

Katz, J. & Smith, A. (2006). Analyzing the HB and HB+ protocols in the "large error" case. *Cryptology ePrint Archive*, 326.

Lee, Y., Batina, L., Singelee, D., & Verbauwhede, I. (2010). Low-cost untraceable authentication protocols for RFID. In *Proc. 3rd ACM Conf. WirelessNetw. Secur. (WiSec'10)* (pp. 55–64). ACM.

Lee, Y., Batina, L., & Verbauwhede, I. (2008). EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol. In *Proc. IEEE Int. Conf. RFID* (pp. 97–104). IEEE Press. doi:10.1109/RFID.2008.4519370

Lee, Y. K., Batina, L., & Verbauwhede, I. (2010). Privacy challenges in RFID systems. In *The Internet of Things* (pp. 397–407). Springer.

Li, J., Chen, X., Chow, S. S., Huang, Q., Wong, D. S., & Liu, Z. (2018). Multi-authority fine-grained access control with accountability and its application in cloud. *Journal of Network and Computer Applications*, *112*, 89–96. doi:10.1016/j.jnca.2018.03.006

Li, J., Liu, Z., Chen, X., Xhafa, F., Tan, X., & Wong, D. S. (2015). L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing. *Knowledge-Based Systems*, *79*, 18–26. doi:10.1016/j.knosys.2014.04.010

Li, J., Sun, L., Yan, Q., Li, Z., Srisa-an, W., & Ye, H. (2018). Significant Permission Identification for Machine Learning Based Android Malware Detection. *IEEE Transactions on Industrial Informatics*.

Liao, Y., & Hsiao, C. (2013). A secure ECC-based RFID authentication scheme using hybrid protocols. In *Advances in Intelligent Systems and Applications* (pp. 1–13). Berlin, Germany: Springer-Verlag. doi:10.1007/978-3-642-35473-1_1

Lin, Q., Yan, H., Huang, Z., Chen, W., Shen, J., & Tang, Y. (2018). An ID-based linearly homomorphic signature scheme and its application in blockchain. *IEEE Access*, *6*, 20632–20640. doi:10.1109/ACCESS.2018.2809426

Luo, H., Wen, G., Su, J., & Huang, Z. (2018). SLAP: Succinct and Lightweight Authentication Protocol for low-cost RFID system. *Wireless Networks*, *24*(1), 69–78. doi:10.1007/s11276-016-1323-y

Mujahid, U., Najam-ul-Islam, M., Jafri, A. R., Qurat-ul-Ain, & Ali Shami, M. (2016). A new ultralightweight rfid mutual authentication protocol: Sasi using recursive hash. *International Journal of Distributed Sensor Networks*, *12*(2), 9648971.

Mujahid, U., Najam-ul-Islam, M., & Sarwar, S. (2017, June). Muhammad Najam-ul-Islam, Shahzad Sarwar, 2017. A New Ultralightweight RFID Authentication Protocol for Passive Low Cost Tags: KMAP. *Wireless Personal Communications*, *94*(3), 725–744. doi:10.1007/s11277-016-3647-4

Mujahid, U., Najam-ul-Islam, M., & Shami, M. A. (2015). RCIA: A new ultralightweight RFID authentication protocol using recursive hash. *International Journal of Distributed Sensor Networks*, *11*(1).

Mukharjee, A. (2015). Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proceedings of the IEEE*, *103*(10).

Ohkubo, M., Suzuki, K., & Kinoshita, S. (2003). Cryptographic approach to privacy-friendly tag, In *Proc. of RFID Privacy Workshop*. Academic Press.

Okamoto, T. (1992). Provably secure and practical identification schemes and corresponding signature schemes. In Proc. Adv. Cryptol. (CRYPTO'92) (pp. 31–53). Academic Press.

Sadighian, J. & Flmap, R. (2008). A fast lightweight mutual authentication protocol for rfid systems. In *Proceedings of the 16th IEEE International Conference on Networks (ICON 2008)*. IEEE Press. doi:10.1109/ICON.2008.4772592

Safkhani, M., & Bagheri, N. (2016). Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. *Cryptology ePrint Archive*, 838. Retrieved from http://eprint.iacr.org/2016/838

Safkhani, M. & Bagheri, N. (2018). Generalized desynchronization attack on UMAP: Application to RCIA, KMAP, SLAP and SASI+ protocols.

Saleem, K., Zeb, K., Derhab, A., Abbas, H., AlMuhtadi, J., Orgun, M. A., & Gawanmeh, A. 2016. Survey on cybersecurity issues in wireless mesh networks based Healthcare. In *Proceedings of the IEEE 18th International Conference on eHealth Networking, Applications and Services (Healthcom)*. IEEE Press.

Schnorr, C. (1989). Efficient identification and signatures for smart cards. In Proc. Adv. Cryptol. (CRYPTO'89) (pp. 239–252). Academic Press.

Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y. (2018). Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *Journal of Network and Computer Applications*, *106*, 117–123. doi:10.1016/j.jnca.2018.01.003

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead, Elsevier. *Computer Networks*, *76*, 146–164. doi:10.1016/j.comnet.2014.11.008

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964–975. doi:10.1016/j.future.2016.11.031

Tewari, A., & Gupta, B. B. (2016). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *The Journal of Supercomputing*, 1–18.

Tian, Y., Chen, G., & Li, J. (2012, May). A New Ultralightweight RFID Authentication Protocol with Permutation. *IEEE Communications Letters*, *16*(5), 702–705. doi:10.1109/LCOMM.2012.031212.120237

Tsudik, G. (2006). YATRAP yet another trivial RFID authentication protocol. *Proceedings of the International Conference on Pervasive Computing and Communications* (pp. 640-643). Academic Press.

Tsudik, G. 2007. Family of dunces: trivial RFID identification and authentication protocols, In *Proceedings of the Symposium on Privacy-Enhancing Technologies* (pp. 45-61). Academic Press. doi:10.1007/978-3-540-75551-7_4

Tuyls, P., & Batina, L. (2006, February). RFID-tags for anti-counterfeiting. In *Cryptographers' Track at the RSA Conference* (pp. 115-131). Springer. 10.1007/11605805_8

Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Security and privacy aspects of low-cost radio frequency identification systems. In *Security in pervasive computing* (pp. 201–212). Springer.

Wolkerstorfer, J. 2005. Is elliptic-curve cryptography suitable to secure RFID tags? In *Proc. Workshop RFID Light-Weight Cryptogr.* (pp. 11–20). Academic Press.

Zhuang, X., Zhu, Y., & Chang, C. (2014). A new ultralightweight RFID protocol for low-cost tags: R 2 AP. *Wireless Personal Communications*, *79*(3), 1787–1802. doi:10.1007/s11277-014-1958-x

Zhuang, X., Zhu, Y., Chang, C.-C., & Peng, Q. (2018). Security Issues in Ultralightweight RFID Authentication Protocols. *Wireless Personal Communications*, *98*(1), 779–814. doi:10.1007/s11277-017-4895-7

Aakanksha Tewari is a Ph.D. Scholar in the Department of Computer Engineering at National Institute of Technology (NIT), Kurukshetra, India. Her research interest includes Computer Networks, Information Security, Cloud Computing, Phishing Detection, Internet of Things, RFID authentication and Number theory and Cryptography. She has done her M. Tech. (Computer Engineering) from Department of Computer Engineering at National Institute of Technology (NIT), Kurukshetra, India. She has participated and won in various National Workshops and Poster presentations. Currently her research work is based on security and privacy in IoT networks and mutual authentication of RFID tags.

B. B. Gupta received PhD degree from Indian Institute of Technology Roorkee, India in the area of information security. He has published more than 200 research papers in international journals and conferences of high repute. He has visited several countries to present his research work. His biography has published in the Marquis Who's Who in the World, 2012. At present, he is working as an Assistant Professor in the Department of Computer Engineering, National Institute of Technology Kurukshetra, India. His research interest includes information security, cyber security, cloud computing, web security, intrusion detection, computer networks, and phishing.