RFID Authentication Protocol for mobile readers satisfying EPC-C1-GEN2 standard of Passive Tags

Y. J. Priyanka
Dept. Computer Science Engineering
National Institute of Technology, Rourkela
Rourkela, India
713cs2047@nitrkl.ac.in

Ashok Kumar Turuk
Dept. Computer Science Engineering
National Institute of Technology, Rourkela
Rourkela, India
akturuk@nitrkl.ac.in

***Abstract*— Radio Frequency Identification (RFID) applications have gained a lot of popularity using which the products can be uniquely identified using the radio signals. With the advancement of technology, the need for mobile RFID readers have been increased rapidly. A lot of RFID authentication protocols have been proposed and most of them have considered the channel between reader and server as secure and also most protocols requires high computational power for RFID tags and according to EPC Class-1 Generation-2 standards of passive tags the one-way hash functions are difficult to compute for passive tags. This paper presents an efficient authentication protocol for mobile RFID readers where an insecure channel is considered between server and reader and also at the same time it can be used for low cost RFID tags. In the proposed protocol authentication is achieved by using low cost cryptographic functions such as a combination of XOR and Pseudo Random Number Generator. The simulation of this protocol is done using AVISPA tool and the security analysis of this proposed protocol is analyzed and hence is proved to be resistant to eavesdropping, replay attack, desynchronization attack, reader impersonation, tag impersonation, traceability and also man-in-the-middle attacks.**

Keywords—security, authentication, cryptography, attacks

I. INTRODUCTION

Radio Frequency Identification (RFID) is used in particular to uniquely identify the objects which has the RFID tags attached to them that uses radio signals to communicate. The RFID system generally consists of three main components that are RFID tags, RFID readers, and a backend server. Each tag has an Electronic Product Code (EPC) associated with it which is unique and thus helps to identify the objects uniquely. The data between reader and tag is exchanged through radio signals. However the security and privacy of the tags have been the main issue as the messages can be eavesdropped by an adversary since all the communications take place through an insecure channel.

The two types of architectures considered in RFID mutual authentication schemes are: one with server and the other is server-less authentication [1, 2, 3]. In the server-based RFID authentication architecture a secure back-end server exists which stores the tag data. To identify a particular tag, the reader communicates with tag through the insecure medium and then send the response to the server through a secure medium. Then the back-end server with the help of stored secret values of tag verifies and authenticates. In case of a server-less RFID authentication, the reader first communicate with a Certificate Authority which then sends the Access List (AL) to the reader which contains the details of all the tags that are accessible by the reader and their corresponding secrets encrypted. In this way the readers can authenticate the tags offline without the involvement of server.

But with the increasing technologies there is a great demand for mobile RFID readers where the readers can be mobile and access the tags within their range without the attached back-end server. In this the communication between reader and server is also through an insecure medium. Thus the security of the authentication protocols should be further improved and only the authenticated readers should be given access to the tags.

The tags are classified as passive, semi passive and active tags according to the way they are powered. The most commonly used tags are passive tags. So in this paper, we have considered passive tags which has no internal power and are powered from the radio signals from the reader while querying the tag.

Also, most of the RFID authentication protocols proposed till date includes high cost computation such as hash functions but according to the Electronic Product Code(EPC) Class-1 Generation-2 standard for passive RFID tags which has been proposed recently, the storage space and computational power of the passive tags is so less that it cannot use high cost cryptography functions and can instead use a combination of small cryptography functions like the bit-wise operations, pseudo random numbers, cyclic redundancy check etc.[6, 7, 10] which are also the built in functions of the passive tags.

So in our proposed protocol we provide RFID authentication in case of mobile readers assuming the channel between reader and server is insecure and the one between reader and tag is also insecure. We have designed this authentication protocol in such a way that it satisfies the EPC-C1-GEN2 standard for passive RFID tags thus making it adaptable to all types of tags.

The rest of the paper is organized in the following way: In section II, we have discussed all the previous work that has been done in the research field of RFID authentication and why is there a need for new authentication protocol. In section III, the entire description of the proposed protocol is mentioned. In section IV, the security analysis of the proposed protocol is stated and in section V, the performance analysis and the comparison of this scheme with others is done. Finally the conclusions will be highlighted in section VI.

978-1-5386-4581-9/18/$31.00 ©2018 IEEE

II. RELATED WORK

In recent years some researchers have worked on RFID authentication protocols. Few of which are presented here.

In 2015, Srivastava [4] has proposed a protocol which is observed to be secure but they have assumed the channel between reader and server to be secure. So, this cannot be used in case of mobile RFID readers and also it cannot be used for passive tags. Later, Erguler, Imran [5] have proposed a protocol considering the insecure channel between reader and server which is observed to be secure. But because of the use of heavy cryptography functions by the tags, this protocol is not ideal for passive tags.

In 2017, Namin [6] proposed a lightweight protocol that can be used by the passive tags since they have used simple cryptography functions like xor and PRNG but they have not considered the computations between reader and server so this cannot be ideal in case of mobile RFID readers.
Later, Tewari [7] has also proposed a lightweight authentication protocol which can be used by the passive tags as they have used a combination of xor and rotation but like in [6] they have not considered the server so this is also not ideal for mobile RFID readers.
Later in the same year, Li, Jing [8] have proposed an ideal protocol for mobile RFID readers which also satisfies EPC-C1-GEN2 standards of passive tags but it is a bit more complex in computations for server side so the overall communication time is a little greater than expected.
After that, Gope, Prosanta [9] have considered the insecure channel between reader and server but used a combination of xor and hash functions because of which it cannot be used for passive tags.

Based on the previous studies mentioned above, we have proposed a new authentication protocol considering both mobile RFID readers and passive RFID tags which is described in the next section.

III. THE PROPOSED PROTOCOL

In this section, we propose a far more efficient RFID authentication protocol in case of mobile RFID readers as shown in Fig.1 in which first the reader authenticates itself to the server before communicating with the tag and thus providing access only to the authorized readers. In this protocol, a combination of xor and pseudo random number generator are used in computing the messages thus avoiding replay attacks and tracing attacks as each message is associated with a freshly generated random numbers. After each successful authentication the secret key of the tag is updated to avoid tag tracing and also both the old and new secret key are stored at the tag side to avoid desynchronization attack. Furthermore, it is resistant to tag impersonation, man in the middle attacks and other common attacks [12].

The notations used in this paper are as follows:

S	: The Server
R	: A mobile RFID Reader
T	: An RFID Tag
RIDi	: ID of an ith Reader
TIDj	: ID of a jth Tag
P_R, P_S	: Public key of reader and server
Pr_R, Pr_S	: Private key of reader and server
N_R, N_T	: Random numbers generated by reader and tag
Sk	: Session key between Reader and Tag
K_T	: Secret key of the Tag
Hash ()	: Hash Function
PRNG ()	: Pseudo Random Number Generator function
$\oplus$	: Bitwise XOR operation
X^{-1}	: old value of X where $X \in \{K_T, Sk, N_R, N_T\}$
AL	: Access List at the server database
{Data}_K	: Encryption/Decryption

A. Assumptions

Our scheme works under the following assumptions:

- The communication channel between reader and server isconsidered to be insecure.
- The reader and tag stores the previous session key values which are used as a secret during their communications.
- The secret key of the tag is known only to tag and the server.
- The authentication between reader and server is achieved by public key authentication and digital signature mechanisms.
- The PRNG() function used is assumed to be known to adversary but the parameters used are kept as secret.

B. Detailed Description of the Protocol

STEP 1: {Reader → Server}
The reader R with ID RID, first generates a random number N_R and computes the message M_1 = {RID, TID, (RID, N_R)_Pr_R}_P_S} which is encrypted using private key of the reader and then public key of the server and is then sent to Server S.

STEP 2: {Server → Reader}
The server on receiving M_1 decrypts the message and checks if RID is an authorized reader and if this Reader has access to Tag TID. If yes, it then computes a message M_2 = PRNG($N_R \oplus K_T \oplus$TID) for Tag and then sends the message $M_3 = \{M_2, \{Hash(RID, N_R)\_Pr_S\}\_P_R\}$ to Reader R.

STEP 3: {Reader → Tag}
The reader on receiving this message M_3 , decrypts it and check if $Hash(RID, N_R)$ matches. If yes then it authenticates the server and then extracts the message M_2 and now it computes M_4= $N_R \oplus$ PRNG (TID $\oplus$ Sk) where Sk is the previous session

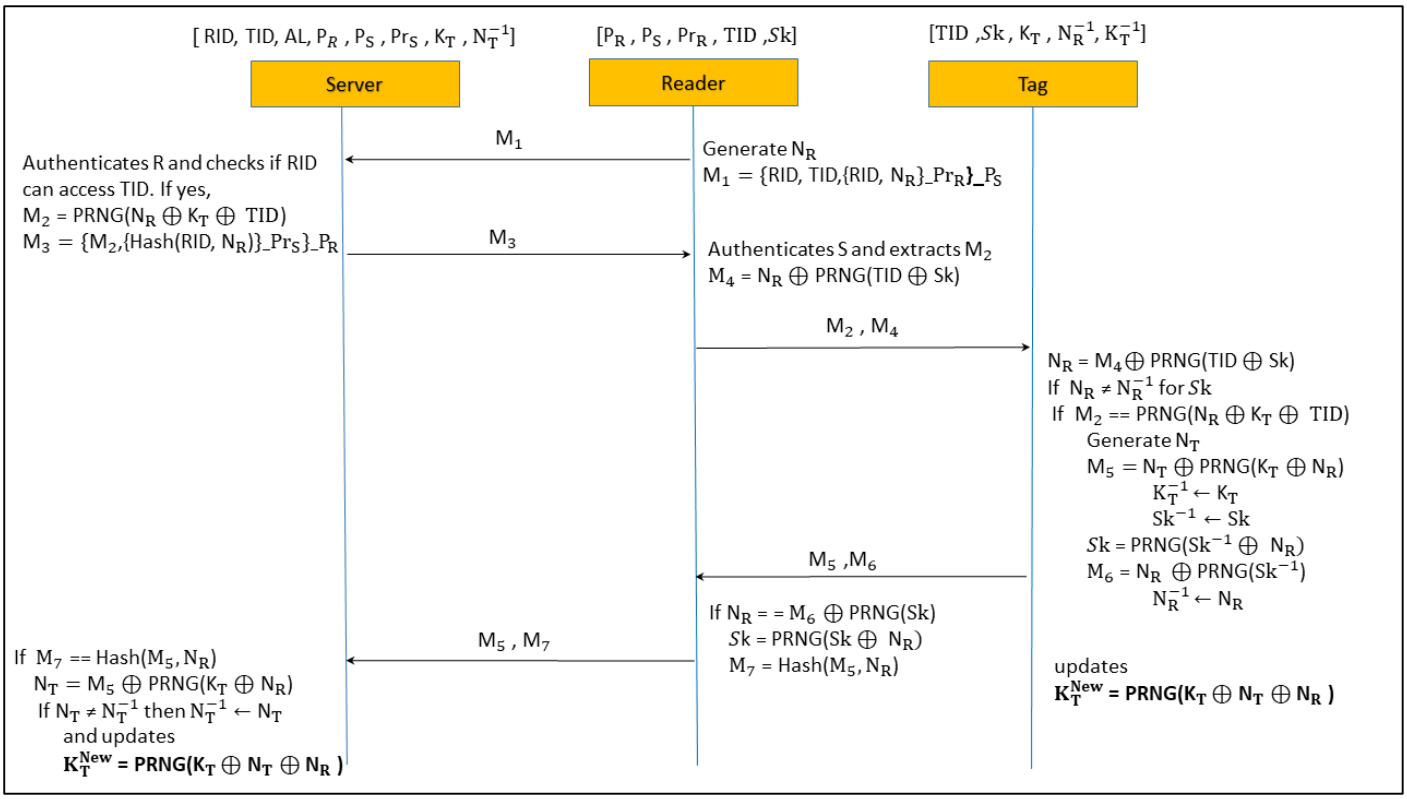

Fig. 1. A mobile reader RFID authentication protocol for passive tags

key which serves as a secret between Reader and Tag. The reader now sends M_2 and M_4 to the Tag T.

STEP 4: {Tag →Reader}
The tag on receiving these messages, gets N_R= $M_4 \oplus$ PRNG (TID $\oplus$ Sk) and checks if this N_R is not equal to previous one that is N_R^{-1} thus confirming its not a replay attack. Using this N_R it checks if M_2 is equal to PRNG ($N_R \oplus K_T \oplus$TID). If yes, then it's an authorized reader and now the tag generates a random number $N_T$and computes M_5 = $N_T \oplus$ PRNG ($K_T \oplus N_R$) for Server and updates its session key Sk = PRNG ($Sk^{-1} \oplus N_R$). It then computes M_6=$N_R \oplus$ PRNG (Sk^{-1}) and sends it to Reader R along with M_5.
After this the Tag stores the secret key into old secret key K_T^{-1} to avoid desynchronization attack and stores N_R into previous number $N_R^{-1}$and then updates new secret key of the tag to K_T = PRNG ($K_T \oplus N_T \oplus N_R$).

STEP 5: {Reader Server}
The Reader on receiving the messages, checks if N_T is equal to $M_6 \oplus$ PRNG (Sk). If yes, then it's a response from a valid Tag and sets the new session key Sk to Sk = PRNG (Sk $\oplus$ N_R). Now it computes M_7= Hash (M_5, N_R) and sends $M_5$and M_7 to Server S.

STEP 6: The server on receiving these messages checks if M_7 is equal to Hash (M_5, N_R) and by this it confirms this message is from the authenticated Reader and now extracts N_T from $M_5 \oplus$ PRNG($K_T \oplus N_R$) and if $N_T$is not equal to N_T^{-1} then it confirms its not a replay attack and now stores N_T^{-1} = N_T .
It then updates the secret key of the tag to K_T = PRNG ($K_T \oplus N_T \oplus N_R$).

IV. Security Analysis

In this section, first we present the security analysis on the AVISPA tool and then the informal analysis is represented.

A. Security Analysis based on AVISPA tool

Automated Validation of Internet Security Protocol (AVISPA) [11] tool which is one of the automated tools available to evaluate and verify the security properties of protocols is used. It performs a real analysis of the security protocol which is written in high level protocol specification language (HLPSL). We have used AVISPA tool for security analysis using OFMC and CL-ATSE back-ends for simulation for our protocol analysis.

Fig.2 represents the output of the proposed protocol on AVISPA tool using OFMC back end.

B. Informal Security Analysis

We have analyzed our protocol against the most common attacks for an RFID authentication protocols such as eavesdropping, replay attack, desynchronization attack, reader impersonation, tag impersonation, tag tracking and man in the middle attack.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/propProtocol.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 1.93s
  visitedNodes: 1232 nodes
  depth: 10 plies
```

Fig. 2. Output of Proposed Protocol on AVISPA tool using OFMC back-end

The detailed analysis is as shown in the following:

- **Eavesdropping:** In our protocol, the complete information of a tag TIDj is stored in the backend server S, which is assumed to be secure. All the message transmissions even if eavesdropped by an intruder, the information cannot be obtained as we have used a combination of random numbers and xor functions along with the secrets. So, the eavesdropper cannot obtain the secret key of the tag or other secrets from those messages. Thus, this proposed protocol is secure against eavesdropping.
- **Replay attack:** If the messages M_2 and M_4 are replayed then the tag identifies the attack because the old random number N_R^{-1} is stored and will be identified and also each message is changed by the random numbers N_R and N_T each time. So, these messages if reused in other sessions, they will be detected. Thus, our protocol is secure against replay attack.
- **Desynchronization attack:** Suppose the messages M_5 and M_7 are not received by the server S, then in the next transition the server computes using the old key K_T^{-1} and sends to the Tag. Since in this protocol the Tag stores both the old and new secret keys after updation, it then uses the old value K_T^{-1} for checking the messages. So, this protocol is resistant to desynchronization attack.
- **Reader impersonation:** Since the private key of the reader is only known to the reader the message transmissions between reader and server can be taken place only by an authorized reader and also since the previous session key between tag and reader is only known to the reader and tag, the tag can identify if it's a fake reader. So, this protocol is secure against reader impersonation attack.
- **Tag impersonation:** Since the previous session key between reader and tag and the secret key of the Tag is only known to the original tag, the tag impersonation or tag cloning is not possible and can be identified by the reader and the server with the messages sent. Thus, this proposed protocol is secure against tag impersonation attack.
- **Tag tracking:** The response of the Tag TIDj is anonymous as the random numbers N_R and N_T, and Sk and K_T ares changed after every successful authentication. So, the eavesdropper cannot distinguish between one response with another from the tag with another. Thus, the location of the tag is difficult to trace. Also, since the updation of Sk and K_T takes place with the combination of secrets and random numbers with the PRNG (), so it would not be possible to find a relation between the forward key and the backward key thus, the forward and backward traceability cannot be achieved.
- **Man In the Middle attack:** Since every message is a combination of pseudo random number along with the secrets, so active eavesdropping or the man in the middle attack cannot be existed even if there is an intruder who is trying to modify the data and sent it to the other party since this can easily be identified and the entity thus stops responding to this intruder. Thus, our proposed protocol is resistant to man in the middle attack.

V. Performance Analysis

The computational cost, the performance and the attacks our proposed protocol is resistant to are compared with other recent protocols proposed by different authors and the results are displayed in the table formats.

TABLE I specifies the transmissions and the methods used by the protocols.

TABLE II specifies the total no of computations used by Server(S), Reader(R) and Tag(T) and it can be clearly seen that our protocol uses simple cryptography functions by the tag to provide security and the server and reader having high computational power can use hash functions.

In TABLE III all the security properties are compared.

TABLE I. Comparison of Transmission and Functionality

	Namin [6]	**Srivastava [4]**	**Erguler [5]**	**Tewari [7]**	**Gope [9]**	**Proposed Protocol**
Methodology used	XOR/ PRNG	Hash/ XOR	Hash/ Encryption	XOR/ Rotation	XOR/ Hash	XOR/ PRNG
Total number of rounds	-	5	7	-	4	5
Insecure channel between R and S	✗	✗	✓	✗	✓	✓
EPC-C1-GEN-2 standard	✓	✗	✗	✓	✗	✓
Number of R and T communications	2	3	3	4	2	2
Number of R and S communications	Not specified	2	2	Not specified	2	3

TABLE II. COMPARISON OF COMPUTATION FUNCTIONS USED

	Namin [6]			Srivastava [4]			Erguler [5]			Tewari [7]			Gope [9]			Proposed Protocol		
Functions used	**S**	**R**	**T**	**S**	**R**	**T**	**S**	**R**	**T**	**S**	**R**	**T**	**S**	**R**	**T**	**S**	**R**	**T**
XOR	NS	11	11	7	-	8	-	-	-	NS	-	-	4	1	3	6	4	10
PRNG	NS	4	4	-	-	-	-	-	-	NS	6	6	-	-	-	3	3	6
Rotation	NS	-	-	-	-	-	-	-	-	NS	-	-	-	-	-	-	-	-
Hash	NS	-	1	5	-	5	6	2	4	NS	-	-	5	2	7	2	2	-
Encryption / Decryption	NS	-	-	-	-	-	4	4	-	NS	-	-	-	-	-	2	2	-

NS: Not specified

TABLE III. COMPARISON OF SECURITY PROPERTIES

	Namin [6]	Srivastava [4]	Erguler [5]	Tewari [7]	Gope [9]	Proposed Protocol
Eavesdropping	✓	✓	✓	✓	✓	✓
Replay attack	✓	✓	✓	✓	✓	✓
Desynchronization attack		✓	✓	✓	✓	✓
Reader impersonation attack			✓		✓	✓
Tag impersonation attack	✓	✓	✓	✓	✓	✓
Tag tracing	✓	✓	✓	✓	✓	✓
Man-in-the-middle attack		✓	✓	✓		✓

VI. CONCLUSION

In this paper, we proposed an RFID authentication protocol for mobile RFID reader with insecure communication channels between reader and server and between reader and tag. The server and reader authenticate themselves with the help of public key encryption and hence can be used in a multiple reader environment. Also, we have designed this protocol in such a way that it satisfies the EPC class-1 generation-2 standard for passive RFID tags since we have used simple cryptography functions which can be easily computed by the passive tags. Then, the security analysis of this protocol is presented both formally with the simulation results using AVISPA tool and informally by describing the attacks that the protocol is resistant to and finally the comparison results of this protocol with other protocols is also presented.

REFERENCES

[1] C.-F. Lee, H.-Y. Chien, and C.-S. Laih, "Server-less rfid authentication and searching protocol with enhanced security," *International Journal of Communication Systems*, vol. 25, no. 3, pp. 376–385, 2012.

[2] C. C. Tan, B. Sheng, and Q. Li, "Secure and serverless rfid authentication and search protocols," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1400–1407, 2008.

[3] J. Li, Z. Zhou, and P. Wang, "Server-less lightweight authentication protocol for rfid system," in *International Conference on Cloud Computing and Security*. Springer, 2017, pp. 305–314.

[4] K. Srivastava, A. K. Awasthi, S. D. Kaul, and R. Mittal, "A hash based mutual rfid tag authentication protocol in telecare medicine information system," *Journal of medical systems*, vol. 39, no. 1, p. 153, 2015.

[5] I. Erguler, "A potential weakness in rfid-based internet-of-things systems," *Pervasive and Mobsile Computing*, vol. 20, pp. 115–126, 2015.

[6] M. E. Namin, M. Hosseinzadeh, N. Bagheri, and A. Khademzadeh, "A secure search protocol for lightweight and low-cost rfid systems," *Telecommunication Systems*, pp. 1–14, 2017.

[7] A. Tewari and B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for iot devices using rfid tags," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1085–1102, 2017.

[8] J. Li, Z. Zhou, and P. Wang, "Cryptanalysis of the lmap protocol: A low-cost rfid authentication protocol," in *Control And Decision Conference (CCDC), 2017 29th Chinese*. IEEE, 2017, pp. 7292–7297.

[9] P. Gope, R. Amin, S. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving rfid authentication scheme for distributed iot infrastructure with secure localization services for smart city environment," *Future Generation Computer Systems*, 2017.

[10] S.-Y. Chiou and S.-Y. Chang, "An enhanced authentication scheme in mobile rfid system," *Ad Hoc Networks*, vol. 71, pp. 1–13, 2018.

[11] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P.-C. Heam, O. Kouchnarenko, J. Mantovaniet al., "The avispa tool for the automated validation of internet security protocols and applications," in *International conference on computer aided verification*. Springer, 2005, pp. 281–285.

[12] M. El Beqqal and M. Azizi, "Classification of major security attacks against rfid systems," in *Wireless Technologies, Embedded and Intelligent Systems (WITS), 2017 International Conference on*. IEEE, 2017, pp. 1–6.