Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology
e-ISSN: 2393-9877, p-ISSN: 2394-2444
(Special Issue for ITECE 2016)

SECURE ULTRALIGHTWEIGHT CRYTOGRAPHY FOR RFID PASSIVE TAG: A SURVEY

Priyanka Pandey[1], Chandresh D. Parekh[2]

[1]*M.Tech. (Cyber Security), Raksha Shakti University, Ahmedabad*
[1]*priyankapandey016@gmail.com*
[2]*Assistant Professor (TC) Raksha Shakti University, Ahmedabad*
[2]*cdp_tc@rsu.ac.in*

Abstract — RFID system is one of the fastest growing technologies among the automation applications needed in Organizations, Institution, and Supply Chain Management etc. Along with non-line of sight capability, RFID tag's capability of durability, reusability, data encryption, increased storage and faster read rate etc. makes RFID systems much efficient, faster and robust than other existing systems such as barcodes, magnetic taps etc. The UMAPs are very important to the widespread deployment of low-cost RFIDs. The UMAPs protocol is vulnerable against traceability attack and forward traceability attack and many others as attacker uses loopholes arises from the extremely small memory and very limited calculating power of tags and by using on-tag ultralightweight operations, which includes the cyclic redundancy check, the exclusive-or, the random number generation, the pseudo random number generator (PRNG) and lightweight cryptographic hash function operations attacker carries out different attacks. This weakness present in UMAPs protocol also does not provide the security and privacy of RFID users. We are taking some UMAP protocol like Yu-Jehn protocol, LMAP, EMAP and others for a survey to study and find the vulnerabilities in these protocols along with the comparison table. This paper shows review of all UMAP protocols and vulnerabilities of all the protocols.

Keywords: Mutual Authentication, RFID, Traceability Attack, Ultralightweight Protocol, UMAPs, Vulnerabilities.

I. INTRODUCTION

RFID is a more specific category which comes under Internet of Thing. RFID is a system in which consists of three main things: a Tag, a Reader and Database called Back-end server. The ID for communication with the Reader is stored in the Tag. The Back-end server consists of a complete database of identification information of all the Tags and the Readers. Readers are allowed to change or add some input to the data received from the Tag and forward it to the Back-end server depending on the type of UMAP protocol used for a particular RFID system.

We have to assume the communication link or channel between reader and back-end server is as secure as there is no power computation issue, so we can make use of various security relevant solutions to enhance the security of the whole RFID system. This link between tag and reader needs more care as this link is wireless which makes it vulnerable to eavesdropping. As, we have very limited resources at the tag end(due to small size), so to make RFID system practically convenient we have to effectively minimize the price of the tag and then we have to look after these security issues seriously within these limited resources[6].

Considering all the above mentioned limitations, a new field of cryptography known as ultralightweight cryptography which uses ultralight operations, had been introduced way back in 2006. This area specifically had been brought for low cost RFID tags to make them applicable and comparable with its withstanding systems and also it provides different approach for security. We are limited to use only 5-10 K gates for low-cost passive RFID Tags which includes 250-3000 gates exclusively for security purpose[6][8].

II. ULTRALIGHTWEIGHT MUTUAL AUTHENTICATION PROTOCOLS

2.1 Introduction

The main objective of this type of cryptography is to ensure the secure mutual authentication between reader and tag in minimum cost with less storage. Because of this cost efficacy, this type of cryptography is called ultralightweight cryptography and related protocols are called ultralightweight mutual authentication protocols (UMAP).

These protocols contains simple operations (bit wise) like AND XOR, OR etc. as other cryptographic functions like one-way hash functions, require 8K and 11 K logical gates respectively, which makes them practically unfeasible [1][6].

2.2 Classification of Authentication Protocol

Basically authentication protocols between Tag and Reader are of two types, namely Authentication with classic cryptographic primitives and Authentication without classic cryptographic primitives. Other than this, there are mutual authentication protocols which provide confirmation to both reader and the tag that they are communicating with legitimate reader/tag. Chein [1] provided the detailed classifications of authentication protocols focused on classic cryptographic functions that can be used at Tag's end for security purpose. We are providing the whole classification in a tabular form for a close look at the classifications.

TABLE 1: Security Protocols

S.No	Authentication Protocol	Cryptographic Operation
1.	Full-fledged protocols	Standard cryptographic algorithms and solutions, like one way hash functions, symmetric or asymmetric cryptography.
2.	Simple authentication protocols	Random number generator and one-way hash functions
3.	Lightweight protocols	Random number generators and simple functions such as Cyclic redundancy checks (CRC) but cannot use hash functions.
4.	Ultralightweight protocols	Simple bitwise logical operations and even random number generator cannot be used at the tag's side.

III. RELATED WORK

Recently, we know there has been proposed many ultralightweight mutual authentication protocols for RFID systems. The main operation of the protocols involves interchange of pseudonyms like keys between reader and tags and IDS (Identity pseudonym). After this, a random number is forwarded by reader to tag because of issues at tag's end relating to power computations. Then this random number easily improves the diffusion property of the protocols [8].When the authentication session becomes successful both tag and the reader update their pseudonyms using predefined comparable equations at both ends so that it remains secure [1][6][2].

To keep the Desynchronization attacks at bay, some protocols allow space so that they can have a secure storage space of old pseudonyms [3]. Protocols which uses this approach are: EMAP (2006), LMAP (2006), SASI (2007), David-Prasad (2009) GOSSAMER (2009), and RAPP (2012) and Yu-Jehn (2015)[6][7][8]. We present the details of the above mentioned protocols along with the vulnerabilities in a comparative manner so as to get an easy and effective analysis of the protocols keeping the security viewpoint as the main focus.

TABLE 2. Security Comparison of Existing Protocol

S.No.	Protocol	Description	Vulnerabilities	Recent Attacks
1.	LMAP	The protocol is categorized into four steps: Tag identification, Mutual authentication, index-pseudonym update and key update. Tag stores one constant (ID) and five variable (IDS and four keys K1, K2, K3, and K4) are variables, each of 96 bits, variables will be updated in a synchronized manner after each successful run of the authentication protocol.	Information leakage Attacks and basic traceability.	Desynchronization and Full Disclosure Attacks.
2.	EMAP	Efficient mutual authentication protocol was another protocol from UMAP family. Here a new Parity function 'Fp' was added, which is introduced, as vector and built from the parity bits. The rest of the procedure was mostly similar to LMAP explained above.	Desynchronization attacks. If the D and E messages of this protocol is blocked and then the reader will updates its pseudonyms but tag will not and hence becomes vulnerable.	Desynchronization and Full Disclosure Attacks.

3.	SASI	Strong authentication and integrity protocol has similar operational structure as proposed in LMAP and EMAP, but here a new function called Rot (Left cyclic Rotation) has been introduced in SASI, which was way different from Triangular functions (XOR, OR etc.) extensively used in previous protocols[2].	If the message D is repeatedly interrupted then this protocol is vulnerable to Desynchronization and Probabilistic Attack	Desynchronization and Probabilistic Attack
4.	GOSSAMER	Gossamer, introduced two new functions; Double Rotation and MixBits. The internal structure of these functions consists of same conventional triangular functions (Shifting &Addition) but have more powerful diffusion properties on comparison with the uncluttered triangular function.	Vulnerable to Denial of Service (DoS) and Desynchronization Attack.	DoS and Desynchronization attacks.
5.	DAVID-PRASAD	The aim of this protocol was to provide the security within limited resources (Hardware and power computation) [2][6]. It also have space to store previous value of IDS to thwart Desynchronization attacks.	Vulnerable to Desynchronization, Traceability, Full Disclosure and Probabilistic Attack	Traceability and Full Disclosure Attack[4].
6.	RAPP	RFID Mutual Authentication Protocol with Permutation initiated a new function called Permutation; which has been assimilated with XOR operation in all equations present in this protocol. The usage of permutation in RAPP in a smart way helps in avoiding the usage of unbalanced AND & OR operations. RAPP consists of only three operations; Bitwise XOR, Left Rotation, and Permutation.	Poor composition of RAPP messages and poor diffusion properties of the Permutation (Per) function makes it vulnerable to Desynchronization Attack.	Full Disclosure Attack.
7.	YU-JEHN	This Protocol reduce communication, storage, updating and computation overheads and also thwart various attacks, such as the DoS, Forward secrecy, Impersonation, MitM and Replay attacks,. It uses only ultralightweight operations, like the RNG, XOR and LHash.	It has two vulnerabilities : 1.The structure of generating $M1 = Ni \oplus r2$ 2. The way $PIDi$ is used in the updating procedure. Both vulnerabilities leads to Traceability Attacks	Forward and Backward Traceability Attacks[4].

IV. SECURITY MODEL FOR CRYPTANALYSIS LATEST UMAPs

The security of the protocols summarized in Table 2.2 has already been analyzed based on two main features: the working principle of the protocols and countermeasures against attacks. We are providing the security model for cryptanalysis of the most recent UMAPs which are Reconstruction based RFID authentication protocol (R2AP)[8], Improved Protocol by Yu-Jehn and SASI Using Recursive Hash. The working principle of the protocols consists of Mutual Authentication between Tag and Reader, Confidentiality and Integrity of data, Tag Anonymity and Untraceability which will be discussed in detail later and for cryptanalysis we have taken Desynchronization Attack, Full Disclosure Attack, Traceability Attack (Forward and Backward) and Probabilistic attack as all these attack are most common and latest[5][6].

The cryptanalysis will give us more loopholes in the above mentioned protocols and we can easily provide the required improvement in these protocols so that they become more secure [4][7].

The important aspects of the working principle of the protocols are briefly explained in the following:

- **Confidentiality and Integrity of Data:**
  Confidentiality and Integrity of the data transmitted between tag and reader is very important as confidentiality provides the privacy with non-repudiation and integrity provides the belief that the data is genuine and error free.

- **Mutual Authentication:** Mutual authentication is fundamental and important for the better functionality of the protocol, in which the reader authenticates the tag and the tag authenticates the reader. This way mutual authentication ensures that either reader or tag is communicating with a genuine one or not.

- **Tag anonymity & Untraceability:** These two aspects are also very important, since if an attacker successfully recognized a particular tag; then the particular tag can be easily traced which can lead to security lapses in the mobility of the tags.

Now, we will analyze the security model which is reformed for a better analysis compared to [6]. This model consists of four attacks; each attack will provide the security loopholes and other vulnerabilities in the protocols. The detailed explanation of each attack is given following:

- **Desynchronization:** In this attack, the hacker tries to disturb synchronization between the reader and tag. This happens when a hacker successfully adjusts the original reader and tag on different pseudonyms (IDS) values.

- **Traceability:** In this attack, hacker tries to find the particular tag, so that its mobility can be traced easily. This will be possible, only if the hacker successfully blocks the pseudonym updating process; which makes the tag Helpless to randomize its IDS as randomization will provide more security as our OTPs.

- **Full Disclosure:** Also called Tango Attack is the extremely persuasive attack among mentioned because this attack can reveal all the credentials. This attack uses selection of Good Approximations and then combination of Good approximations and these approximations are used only when the attacker already eavesdropped few sessions by intercepting the communication between the reader and tag.
- **Probabilistic/Ad hoc:** This attack is not having a fixed pattern to launch the attack as the name suggests. In this, the loopholes in mathematical equations of the protocols are used by the hacker along with some smart cryptanalysis to reveal the keys and IDs of the tags.

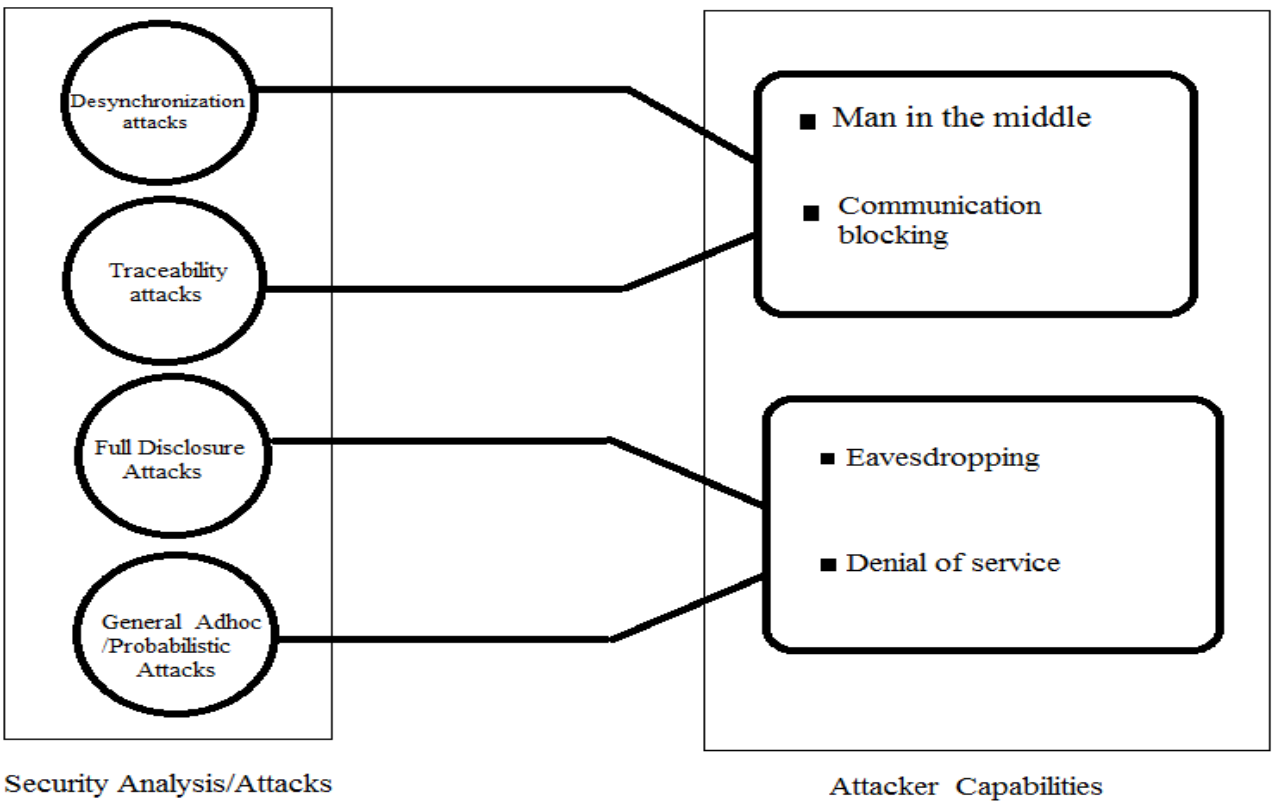

FIGURE 1. Security Model for UMAP

V. CONCLUSION

In this review paper we have gone through existing UMAPs and found vulnerabilities present in them and presented them in an effective manner. To provide more security to these protocols, we have studied each protocol in detail and found the required loopholes which will be considered for cryptanalysis in our future work and this cryptanalysis provide more security to existing protocols. Also we have mentioned the latest protocols which need to be tested through the security model to get more secure protocol. In future, we will focus on latest protocol and do cryptanalysis on them to find existing vulnerabilities.

REFERENCES

[1] Hung-Yu Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 4, NO. 4,pp.337-339.

[2] Muhammad Zakarya, Syed Bilal Hussain Shah, Aftab Alam, "An Overview of New Ultra Lightweight RFID Authentication Protocol SASI ", IJCSI International Journal of Computer Science Issues, Vol. 8,pp.518-523.

[3] R. K. Pateriya, Sangeeta Sharma , 2011 ,"An Ultralightweight Mutual Authentication Protocol for Low Cost RFID passive Tags", International Journal of Computer Applications , Volume 25 – No.10.

[4] Seyed-Salman,Sajjadi Ghaem Maghami, Afrooz Haghbin, Mahtab Mirmohseni, 2015," Traceability Improvements of a New RFID Protocol Based On EPC C1 G2",

[5] Umar Mujahid, M. Najam-ul-Islam, and M. Ali Shami, "RCIA: A New Ultralightweight RFID Authentication Protocol Using Recursive Hash" , Hindawi Publishing Corporation International Journal of Distributed Sensor Networks , 2015, Article ID 642180, 8 pages.

[6] Umar Mujahid ,M. Najam-ul-Islam, "Ultralightweight Cryptography for Passive RFID Systems",in process of International Journal of Communication Networks and Information Security (IJCNIS), Vol. 6, No. 3, December 2014. pp.173-180

[7] Xu Zhuang, Yan Zhu, Chin-Chen Chang, 2014, "A New Ultralightweight RFID Protocol for Low-Cost Tags: R2AP", Wireless Pers Commun, Published online: 26 July Springer Science+Business Media New York.

[8] Yu-Chung Huang, Jehn-Ruey Jiang,20, "Ultralightweight RFID Reader-Tag Mutual Authentication Revisited", in process of IEEE International Conference on Mobile Services,pp.1-173.