RFID Security in the Context of "Internet of Things"

Renu Aggarwal
Dhirubhai Ambani Inst. of Information and Communication Technology
Gandhinagar - 382007
Email: renu_aggarwal@gmail.com

Manik Lal Das
Dhirubhai Ambani Inst. of Information and Communication Technology
Gandhinagar - 382007
Email: maniklal_das@daiict.ac.in

ABSTRACT

Internet has emerged as a medium to connect entities across the world for emailing, conferencing, trading, gaming and so on. Internet of Things (IoT) is emerging as a global network for connecting any objects (physical or virtual) across the globe, ranging applications from home appliances to consumer electronics. In IoT, physical objects such as home appliances, vehicles, supply-chain items, containers, etc. should have unique identities for interacting among themselves. As a result, unique identification of trillion of objects is a foremost requirement in IoT. RFID (Radio Frequency IDentification) technology plays an important role in IoT for solving identification issues of objects around us in a cost effective manner. The usage of low cost RFID tags draws greater attention from researchers in recent past, as the cost of supply-chain items should not exceed much because of embedded tag cost. The communication between tag and reader takes place over insecure channel. Therefore, security concern has become an important issue in RFID systems. In recent years, several light-weight protocols and improvements have been proposed for RFID security. Some of them have succeeded with their security claim, but many protocols suffer from security weaknesses or design flaws. In this paper, we discuss a recently proposed protocol's strengths and weaknesses and then proposed an improved protocol, retaining efficiency of the protocol intact.

Categories and Subject Descriptors

D.4.6 [**Authentication**]: [Security and Protection]

General Terms

Internet of Things, RFID Security

Keywords

Internet of Things, RFID systems, Security, Privacy, Authentication.

1. INTRODUCTION

The term Internet of Things was introduced by Kevin Ashton in 1999. Internet of Things is still evolving and people define the term in different ways. According to authors understanding, Internet of Things (IoT) [1] is a paradigm, where the existing networked devices connect to the real-world objects such as home appliances, vehicles, healthcare and so on. Smart objects (we term objects as things) will be able to sense other objects around them and will be able to communicate to each other using the Internet. Objects include not only the material things but also the virtual things and the events connected to them. IoT extends the communication between human and applications to integrate things within it. IoT can also be considered as a Global network which allows the communication between human-to-human, human-to-things and things-to-things, that is, anything in the world by providing a unique digital identity to each and every object. Therefore, in order to take the desired shape of IoT, every object in the world needs to be connected thorough a unique identity. Radio Frequency IDentification (RFID) technology [1] provides the platform to solve this issue using RFID tag. RFID tag has a unique identification that can be attached/embedded to an object. Use of RFID tags in IoT enable in managing the unique identification for trillions of objects expected to be connected in the IoT. We note that 128-bit IPv6 addressing scheme has been adopted in many applications which can accommodate several trillion addresses [2]. This paper focuses the security issues of RFID system in the context of IoT.

RFID system consists of tag, reader and database (back-end) server. RFID tag and reader can communicate over an insecure channel, typically in short range. The tag is a microchip with memory combined with an antenna, where the antenna picks up signals from an RFID reader and then returns the signal back to the reader with some additional data (e.g. a unique serial number). Every tag has a unique identity (we say, TID), which is a string of bits stored in its memory and used for tag/item identification purpose. For example, information about a product, manufacturing date, expiry date, sell/buy, price, warranty information can be written into the tag. A reader consist of an antenna which emits radio waves through which nearby tags respond to the reader. One or more readers are connected to the back-end server of the RFID systems, which is, typically, a high speed computer securely communicate to readers as and when required. After collecting information from tags, the reader sends data it to the back-end server for tag validation or required data processing. The back-end server is assumed to be a trusted server that maintains all valid tags and readers information in its database.

Types of RFID Tags. Broadly, there are three types of RFID tags.

- Active tag: Active tag is a device which has its own power supply equipment. It can transmit data back to the reader by itself without the reader's emitted signals.

SecurIT'12, August 17-19, 2012, Kollam, Kerala, India

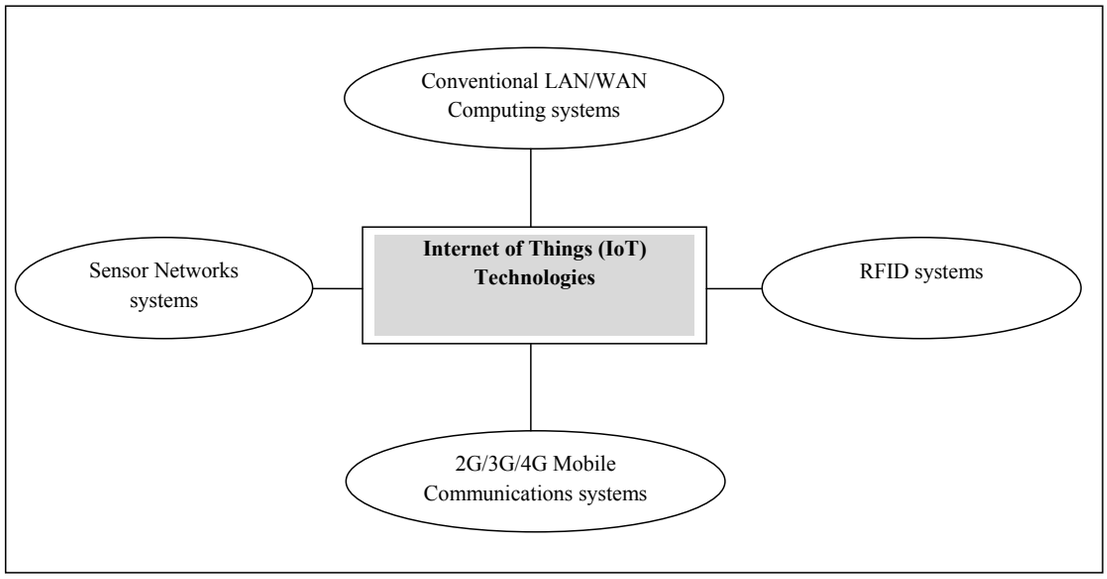

Figure 1: Technologies involved in Internet of Things

- Passive tag: Passive tag has no power supply equipments in it. They are designed to absorb power from the incoming signal from reader in order to energize the circuit and transmit the data stored in its memory back to the reader.

- Semi-active tag: Semi-active tag has its own power supply equipment, but they also absorb power from reader's signal.

Among the above types, passive tags are more economical and popular because of their longer lives and low manufacturing cost. Because of resource limitation of tags, RFID system typically supports light-weight security solution for authentication and authorization. The problem with RFID security is that the tag has limited computational capabilities, consequently, conventional symmetric (e.g. Advanced Encryption Standard) and asymmetric cryptographic primitives (e.g. RSA algorithm) are not practical at the present scenario of RFID systems. Therefore, protocols that involve bitwise exclusive-OR (XOR) and hash operations are in high demand in industry and will also be suitable for IoT, as communication between RFID tags and sensors require light-weight security solution because of its resource-constrained environment.
RFID tags are small and thus, can be attached to consumer goods, library books, home appliance items for identification and tracking purposes. However, the object tracking mechanism can be misused by bad guys. Object tracking which is RFID tag-enabled has both plus and minus points. The plus points are tracking missing/stolen items and locating criminals. Whereas, minus points are compromising privacy of item/tag owner, unnecessary disturbance to persons who is carrying items. As a result, security and privacy issues of RFID system are important concerns and require more attention from researchers. There have been several light-weight protocols and improvements [3], [4], [5], [6], [7], [8], [9] proposed in literature for RFID security in recent past. However, many of them suffer from security weaknesses or design flaws.

Contributions of this paper. As a part of security and privacy issues of Internet of Things, we discuss a recently proposed light-weight RFID protocol [10]. The protocol is efficient, but suffers from disclosure and desynchronization attacks. We then proposed an improved protocol by mitigating security weaknesses of the protocol in [10], but retaining other features along with efficiency factor of the protocol.

Organization of the paper. The remainder of the paper is organized as follows. Section 2 reviews some important security properties and security goals of RFID systems. Section 3 discusses a recent light-weight protocol for RFID security. Section 4 presents the improved protocol and Section 5 analyses it. We conclude the paper in Section 6.

2. SECURITY AND PRIVACY ISSUES IN RFID SYSTEMS

This section provides an overview of the security issues of an RFID system. An RFID system, typically, aims to achieve following security services.

- *Privacy* - Privacy is one of the main concerns in the RFID systems. The use of radio waves has enabled easy eavesdropping and as a result the information relating to the tag could be an easy target by an adversary.

- *Location Privacy* - If the response of a certain tag can be distinguished from the rest of the tags like responding in the same manner or sending same message in case of desynchronization can lead to the identification of the tag then it is prone to monitoring. In other words, wherever the person carries some item which is embedded with a tag then the item can be tracked down by querying the tag.

- *Mutual authentication* - Mutual authentication ensures legitimacy of tag-reader identification.

2.1 Advantages and Disadvantages of an RFID System

Advantages

An RFID system could provide following advantages:

- Efficiency: RFID tags are low-cost and can be read through plastic, wood and even through human body. The low-cost tag-reader communication enables easy tracking of tag-enabled items.

- Maintainability: RFID system costs more than a barcode system, but provides a good return on investment in a long run, as RFID is significantly more efficient.

- Resistance: RFID tags are less susceptible to damage. An RFID tag is securely placed within an object or embedded in plastic, enabling the system to be used in a variety of harsh environments, such as areas of high temperature or moisture, or with exposure to chemicals or the outdoors.

- Controlling object: With RFID technology, tag-enabled item tracking is done in a controlled manner. In case of any misuse of tags' items, reader can trigger appropriate message to seller/vendor of the items.

- Fault-tolerance: Fault-tolerance is a property that enables a system to continue operating properly in the event of the failure of some of its components. Let's consider following scenario: in a healthcare where patients condition is monitored by RFID systems. If a patient's condition is critical and at that moment the doctor (who is located in a remote area) is unable to communicate the patient's RFID tag then the cost of the fault would become high. The system should provide some sort of solution so that the high risk fault can be controlled with a lifesaving effort.

- Accountability: RFID systems can provide better accountability not only for sell/buy process of products but also for its effective maintenance. The reader can have history of a particular tag for conducting an audit if any needs arise.

- Sustainability: Sustainability is the capacity to endure. Barcode system is basically use-and-throw like system. Once an item is out of stock there is no means to check or diagnose it at a later time through the barcode system. In contrast, RFID systems can sustain for a long tenure. As long as RFID tag of an item is not physically tampered, the tag can communicate to the reader and vice-versa.

- Security: RFID systems provide better security than barcodes in the sense that an RFID system can track, control, update and provide a bridge to other resource-constrained environment like sensor networks.

Disadvantages

Although an RFID system provides above mentioned advantages, the system has some limitations as given below:

- Expensive: RFID systems are typically more expensive than alternatives such as barcode systems. While passive tag reading cost is comparable to barcode reading, active tags are costly due to their complexity.

- Collision: Tag collision and reader collision are common problems in RFID systems. Tag collision occurs when numerous tags are present in a confined area, and reader collision results when the coverage area managed by one RFID reader overlaps with the coverage area of another reader. This causes signal interference and multiple reads of the same tag's information.

- Privacy: Loss of privacy is a major issue in RFID systems. The tag of an object can be monitored wherever the tag-enabled object is active. This has both good and bad points. The good points are - locating a stolen item, getting service from a compliant reader while moving from one place to another, communicating useful information (e.g. traffic flow, patient's condition) in real time, etc. On the other hand, the bad side would be locating tag-enabled object that is placed is a restricted zone, getting access to some other objects through tags, stealing credit card number when tag-enabled object crosses a reader/compliant device without tag owner's knowledge, etc.

- Compatibility: Tag-reader vendor dependency is a bottleneck for the situation where RFID application requires a tag of vendor-A to communicate with a reader of vendor-B. Therefore, tag-reader-vendor database compatibility issues should be minimized for making RFID application more robust and scalable.

- Data eavesdropping: Data eavesdropping by internal or external entities is a concern for RFID systems. An adversary can eavesdrop transmitted data over-the-air and can try to obtain some important data, if the transmitted data does not provide sufficient safeguard or protection. Data misuse or leakage by internal entities is a major threat in any system including RFID where data is stored in a database server.

3. THE CWH PROTOCOL

Chen *et al* [10] proposed an ultra-lightweight RFID protocol using bitwise exclusive-OR and bit-rotate operation. Although the protocol is efficient, it is vulnerable to full disclosure attacks [11], [12], [13]. We briefly describe the protocol and its weakness as follows.

- Reader first generates a 128-bit long random number r. As reader identity (we say, RID) is known to both tag and reader, the random number is XORed with the RID as $s = RID \oplus r$. The reader sends the query along with s to the tag.

- Tag retrieves r by XORing s with RID. It then computes $n = weight(r)$, where the $weight(\cdot)$ function is calculated as follows: the number of '1's (say, n) in the binary string shifts r to the left for n bits generating r'. After that, it computes $t = TID \oplus r'$ and transmits t to the reader which forwards it to the back-end server along with r, where TID is the tag identity.

- The back-end server computes $n = weight(r)$ and obtains r' in the similar manner. It then obtains the *TID* by XORing the message t with r'. If the *TID* is valid then the process gets completed.

3.1 Full Disclosure Attack

The idea behind the Full Disclosure Attack [11], [12], [13] is that the adversary modifies the input to the tag and uses the response from the tag to obtain the secret information of *RID* and *TID*. The adversary intercepts one successful communication between the tag and the reader and obtains s and t. Then the adversary modifies the message s by XORing it with $[I]_0$, where $[I]_0 = [000 : : : 001]$ is a 128 bit number with LSB (Least Significant Bit) equal to binary value '1' and rest of the bits are '0's. The adversary sends the modified input s' to the tag and collects the response from the tag. If the last bit of r is '0' then the new random number generated by XORing s' with the RID will have one more binary value '1' at the LSB position and hence its weight increases by '1' and if LSB is '1' then the weight of new random number decreases by '1'.

$s = RID \oplus r$
$n = weight(r)$
$r' = Rot(r, n)$
$t = TID \oplus r' = TID \oplus Rot(r, n)$ ——————(A)
$r_1 = RID \oplus s_1 = RID \oplus s \oplus [I]_0 = r \oplus [I]_0$
$n_1 = weight(r_1) = weight(r \oplus [I]_0) = n \pm 1$

Therefore, we have

$r'_1 = Rot(r_1, n_1) = Rot(r \oplus [I]_0, n \pm 1)$
$t_1 = TID \oplus r'_1 = TID \oplus Rot(r \oplus [I]_0, n \pm 1)$ ——(B)

Then the attacker sends a new random number s_2 and stores the response t_2 from the tag, where

$t_2 = TID \oplus Rot(RID \oplus s_2, weight(RID \oplus s_2))$

From equations (A) and (B) we have

$t \oplus t_1 = TID \oplus r' \oplus TID \oplus r'_1 = r' \oplus r'_1 = Rot(r, n) \oplus Rot(r \oplus [I]_0, n \pm 1)$

The above information can be used further to obtain the *TID* and the *RID*.

4. THE IMPROVED PROTOCOL

The CWH protocol uses the bit rotation techniques to increase the complexity of the adversary's task to break the protocol. To increase its complexity further, we perform shifting operation on the message $s = r \oplus RID$. As the *RID* is known to both tag and reader, the number of bit value '1' present in it can be used for shifting the bits of message s. However, this can not prevent the disclosure attack, it just increases the complexity. Therefore, we need to include *TID* in the message sent from tag in such a way that even if adversary makes minor changes in the input and uses the response from the tag, he will not be able to obtain any meaningful information. The improved protocol works as follows:

1) Reader generates a 128-bit random number r and computes $s = RID \oplus r$, $n_1 = weight(RID)$
where n_1 is the number of bit value '1' of *RID*. The reader shifts s to the left for n_1 bits and generates s'. After that the reader broadcasts query and s' to the tag.

2) Tag, upon receiving s' and query, obtains the value of s by shifting s' to the right for n_1 bits. The *RID* is already stored in the tag's memory so the tag can recover the random number r by XORing s with *RID*. Then the tag computes $n_1 = weight(r)$, where n_1 is the number of binary value '1' of r. After that, tag shifts r to left for n_1 bits to generate a new number r'. Tag now generates another random number r'_{prev} by rotating r_{prev} to the left for n_1 bits. The value r_{prev} was generated by the tag in the previous session by rotating the random number sent to it in that session by the number of binary value '1' present in it (in the very first session, the tag will use all 0s or all 1s as r_{prev}). The tag keeps updating the value of r_{prev} in every session. It computes $t_1 = (TID \oplus r'_{prev}) + (r' \wedge r'_{prev})$ and transmits it to the reader.

3) The reader forwards the messages t_1 and r to its back-end server for tag's authenticity check. The back-end server computes $n = weight(r)$ and $r' = Rot(r, n)$. The back-end server also maintains a copy of the r_{prev} and computes r'_{prev} in the similar manner as r'. The *TID* is obtained by subtracting the value $(r' \wedge r'_{prev})$ and XORing the result with r'_{prev}. By checking the obtained *TID* and the stored one, the tag's authentication can be ensured. Once tag's authenticity is confirmed, the back-end server computes r'' and r''_{prev} by rotating r' and r'_{prev}, respectively, by number of bit value '1' present in *TID*. Then the server computes $t_2 = (TID + r''_{prev}) \wedge r''$. The server maintains another random number r_{old} which is equal to the value of r_{prev} in the previous session. After calculating t_2, the server updates the value of $r_{old} = r_{prev}$, i.e., the value of r_{prev} in the current session and $r_{prev} = r'$. Here, r_{old} is used to prevent desynchronization attack (explained in next section). The server then sends t_2 to the reader that forwards it to the tag.

4) Tag computes r'' and r''_{prev} in the similar manner using the values stored in its memory and computes t_2' = $(TID + r''_{prev}) \wedge r''$. If t'_2 is equal to t_2, tag sends message to the reader so that the server updates its $r_{prev} = r'$. The message flow of the protocol is depicted in Figure 2.

5. SECURITY ANALYSIS

The proposed protocol is analysed below and shown that it provides mutual authentication of tag and reader, resists discloser attacks and desynchronization attacks. The proposed protocol can also provide other security attributes that the CWH protocol can achieve.

Mutual Authentication. The proposed protocol ensures mutual authentication of tag and reader (with the help of the back-end server). The tag is authenticated by the back-end server through message t_1, where t_1 is

$$t_1 \leftarrow (TID \oplus r'_{prev}) + (r'_{prev} \wedge \text{r'})$$

The tag uses the random number sent to it by the reader and calculates t_1. The back-end server obtains the *TID* only if it comes from a valid tag. The back-end server and reader are authenticated by the tag through message t_2, where t_2 is $t_2 \leftarrow (TID + r''_{prev}) \wedge$ r"

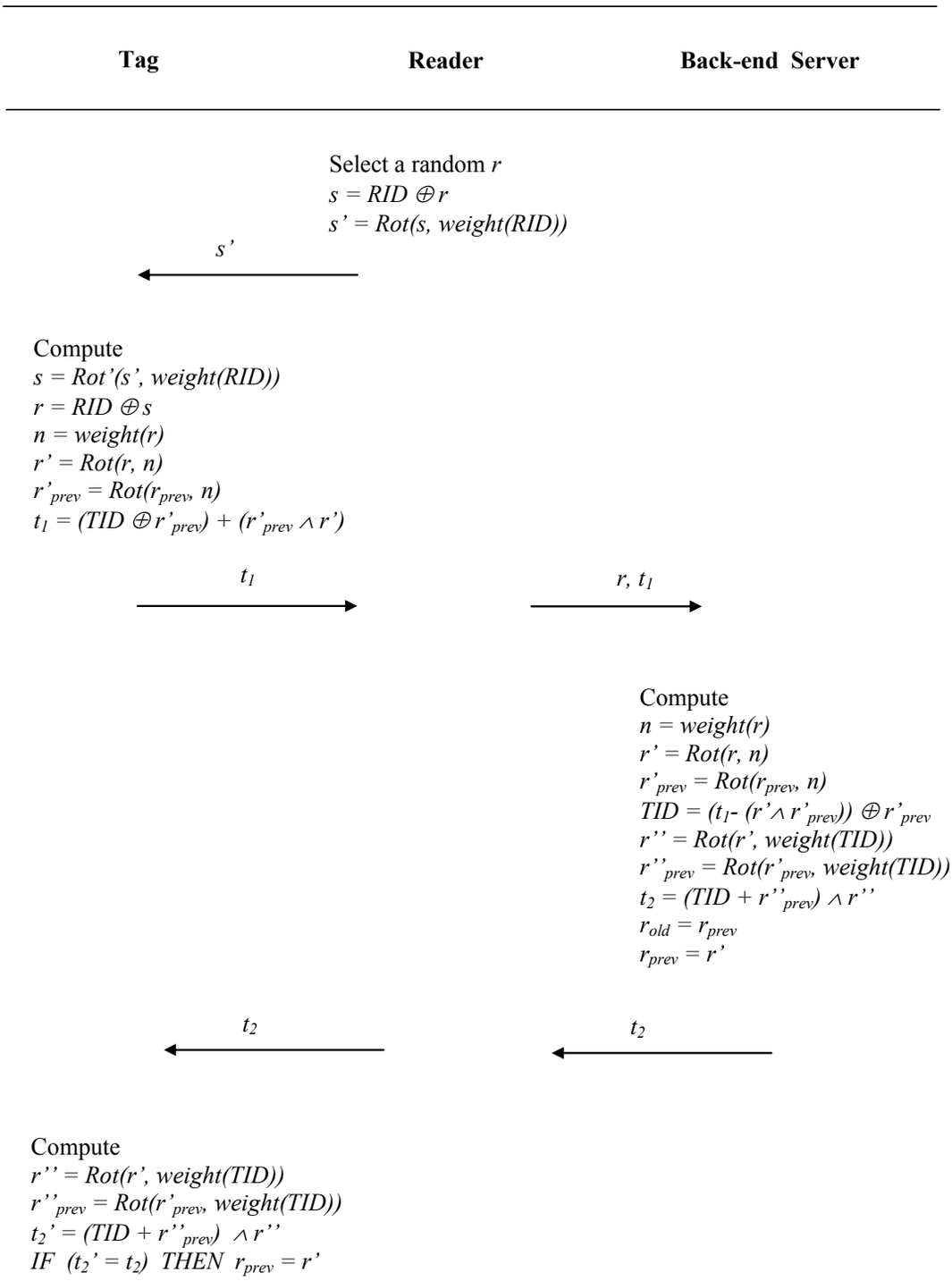

Figure 2: The Message Flow of the Proposed Protocol

It is clear from above that only the genuine back-end server will be able to obtain *TID* from t_1 and then can construct message t_2 which will be validated by the tag. The integrity of the data is also maintained by sending the parameters in a manner that the adversary can not identify or tamper them without being caught. If the adversary tries to alter any message then either tag or back-end server will be able to identify it and terminate the communication.

Resistance to Replay attacks. Every session in the protocol is composed of nonce chosen by the tag and reader.

Suppose that an adversary replays message $s' = Rot(r \oplus RID, weight(RID))$, where r is the random number chosen by the reader. As the tag keeps updating the value of r_{prev} in every session (here, r_{prev} is another random number generated by the tag in the previous session), $t_2 \leftarrow (TID + r''_{prev}) \wedge r''$ sent by the reader would be different from all previous sessions and the adversary would be caught if he tries to replay all the message from the previous session. Similarly, if the adversary tries to replay message intercepted from tag then the authentication process fails because the reader sends another nonce in every session, in tern, message from the tag would be different in every session. Therefore, the protocol resists replay attacks.

Resistance to disclosure attacks. The disclosure attack [13] we discussed in section 3.1 was due to the adversary's ability to obtain a single equation in terms of r (unknown parameter), t and t' (known parameters). In the improved protocol, even if the adversary modifies the message from the reader and uses the response, it still will not be able to remove *TID*. As a result, the protocol can defend the disclosure attack.

Resistance to desynchronization attack. The desynchronization attacks [11], [12], [13] make the back-end server and tag store different values of r_{prev}. The value gets updated by both tag and server after every session. The desynchronization attack is occurred when the adversary prevents the message t_2, sent by the reader, from reaching the tag. In that case, the server might have already updated its r_{prev} value, while on the tag side, since it did not receive the message t_2, the session remains incomplete and tag will not update its r_{prev} value. In the next session, when tag and server communicates, the server calculates *TID* using its r_{prev}. As the value differs from the tag's r_{prev} value, the tag will not be able to perform correctly (fails to authenticate data). In this scenario, the server uses r_{old} value instead of r_{prev} value and passes the authenticating process. If the adversary attempts to attack, aiming that the server changes it r_{old} value, then the attack fails because in the subsequent two sessions the server will be able to identify that r_{prev} needs to be resynchronized with the tag. Therefore, the desynchronization attack fails in the improved protocol.

6. CONCLUSIONS

We have discussed the application and security issues of RFID systems in the context of Internet of Things. Internet of Things emerges as global network, connecting every object around us in near future. However, due to heterogeneous objects in Internet of Things, integration, interoperability and security issues are of primary concerns, which should get more attention from the researchers. As RFID system is going to play a significant role in Internet of Things, we discussed a recent work [10] on light-weight RFID security. The protocol [10] found to be efficient, but it fails to achieve its claimed security, as it suffers from disclosure attacks and desynchronization attacks. We proposed an improved protocol by mitigating the security weaknesses of [10]. The improved protocol is also computationally efficient.

Acknowledgement

This work was carried out while the first author was a 4^{th} year B.Tech. student at Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar. This work is supported in part by Department of Science and Technology, Ministry of Science & Technology, Government of India through DST/INT/SPAIN/P-6/2009 Indo-Spanish Joint Programme of Cooperation in Science and Technology.

7. REFERENCES

[1] L. Yan, Y. Zhang, L. T. Yang and H Ning . Internet of things: from RFID to the next-generation pervasive networked systems. Auerbach Publications, 2008.

[2] The IPv6 Challenge Part 1, A Service Provider guide to the Basics, Transition Strategies, and Implementation Issues. A white paper by Incognito Software, 2011.

[3] D. M. Konidala, Z. Kim and K. Kim. A Simple and Cost-effective RFID Tag-Reader Mutual Authentication Scheme. In proc. of the International Conference on RFID Security, pp. 141–152, 2007.

[4] Y. C. Lee, W. C. Kuo, Y. C. Hsieh and T. C. Chen. Security Enhancement of the Authentication Protocol for RFID Systems. In proc. of the International Conference on Information Assurance and Security, vol.1, pp.521–524, 2009.

[5] H. Y. Chien. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. In: IEEE Transactions on Dependable and Secure Computing, vol. 4, pp.337–340, 2007.

[6] T. Cao, E. Bertino and H. Lei. Security Analysis of the SASI Protocol. In: IEEE Transactions on Dependable and Secure Computing, vol. 6, pp.73–77, 2009.

[7] H. M. Sun, W. C. Ting and K. H Wang. On the Security of Chien's Ultralightweight RFID Authentication Protocol. In: IEEE Transactions on Dependable and Secure Computing, vol. 8, pp.315–317, 2011.

[8] B. Song and C. J. Mitchell. RFID authentication protocol for low-cost tags. In proc. of the ACM Conference on Wireless Network Security, pp.140–147, 2008.

[9] P. Rizomiliotis, E. Rekleitis and S. Gritzalis. Security Analysis of the Song-Mitchell Authentication Protocol for Low-cost RFID Tags. In: IEEE Communication Letters, vol. 13, pp.274–276, 2009.

[10] Y. C. Chen, W. L. Wang, and M. S. Hwang. Low-cost RFID authentication protocol for anti-counterfeiting and privacy protection. In: Asian Journal of Health and Information Sciences, vol. 1, no. 2, pp.189–203, 2006.

[11] H. Y. Chien and C. W. Huang. Security of ultralightweight RFID authentication protocols and its improvements. In: ACM Operating System Review, vol. 41, no. 2, pp.83–86, 2007.

[12] T. Li and G. Wang. Security analysis of two ultralightweight RFID authentication protocols. In proc. of the IFIP Advances in Information and Communication Technology, vol. 232, Springer, pp.109–120, 2007.

[13] T. Cao and P. Shen. Cryptanalysis of Two RFID Authentication Protocols. In: International Journal of Network Security, vol.9, pp.95–100, 2009.