Lightweight Security Enhancement Protocol for Radio Frequency Identification(RFID)

Sumana Basu[1], Debjyoti Paul[2], Sukanya Ghosh[3]

[1]*Computer Science and Engineering, B. P. Poddar Institute of Management and Technology, Kolkata, India*

sumana.basu21@gmail.com

sukanya.mist@gmail.com

[2]*Computer Science and Engineering, Institute of Engineering and Management, Kolkata, India*

debjyotipaul385@gmail.com

***Abstract*— Though RFID provides automatic object identification, yet it is vulnerable to various security threats that put consumer and organization privacy at stake. In this work, we have considered some existing security protocols of RFID system and analyzed the possible security threats at each level. We have modified those parts of protocol that have security loopholes and thus finally proposed a modified four-level security model that has the potential to provide fortification against security threats.**

***Keywords*- RFID, Eavesdropping, Slotted ID, Spoofing, Tracking**

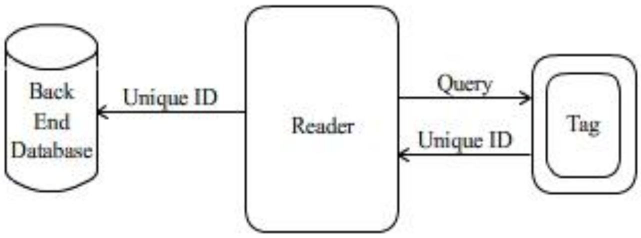

Fig. 1

I. Introduction

Radio Frequency Identification is a generic term for identifying living beings or objects using Radio Frequency. The benefit of RFID technology is that, it scans and identifies objects accurately and efficiently without visual or physical contact with the object [1], [3].

A typical RFID system consists of:

1) An RFID tag
2) A tag reader
3) A host system with a back-end database[2]

Each object contains a tag that carries a unique ID [3]. The tags are tamper resistant and can be read even in visually and environmentally challenging conditions [3] such as snow, ice, fog, inside containers and vehicles etc [2]. It can be used in animal tracking, toxic and medical waste management, postal tracking, airline baggage management, anti-counterfeiting in the drug industry, access control etc. It can directly benefit the customer by reducing waiting time and checkout lines [3] due to its very fast response time. Hence, it should be adopted pervasively.

For low cost RFID implementation, inexpensive passive tags that do not contain a battery [5] and can get activated only by drawing power from the transmission of the reader [4] through inductive coupling are used. Tags don’t contain any microprocessor [6], but incorporate ROM (to store security data, unique ID, OS instructions) and a RAM (to store data during reader interrogation and response) [2], [6].

In the simplest case, on reader interrogation the tag sends back its secret ID (Fig-1). The universally unique ID makes the tag vulnerable towards tracking as it moves from one place to another. This violates “location privacy”. Unprotected tags could be monitored and tracked by business rivals. An ID, if known to an illegal reader could be used to produce fake tags that would successfully pass through security checks in future.

Hence, the security of RFID tags and the stored ID is of extreme importance and sensing the probable security loopholes we have proposed a tag monitoring protocol that would reduce the security threats due to eavesdropping and tracking.

II. Security Threats

A. *Eavesdropping Scenario:*

Eavesdropping normally occurs when the attacker intercepts the communication between an RFID token and authorized reader. The attacker does not need to power or communicate with the token, so it has the ability to execute the attack from a greater distance than is possible for skimming. It is, however, limited in terms of location and time window, since it has to be in the vicinity of an authorized reader when transaction that it is interested in, is conducted. The attacker needs to capture the transmitted signals using suitable RF equipment before recovering and storing data of interest [4], [8].

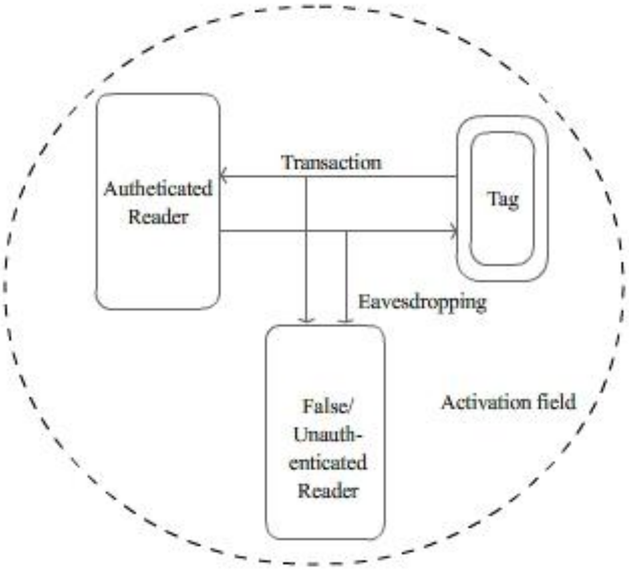

Fig. 2

B. Forward privacy:

Forward privacy ensures that messages transmitted today will be secure in the future even after compromising the tag. Privacy also includes the fact that a tag must not reveal any information about the kind of item it is attached to [9], [10].

C. Spoofing:

It is possible to fool an RFID reader into believing it is receiving data from an RFID tag or data. This is called "SPOOFING". In spoofing someone with a suitably programmed portably reader covertly read and records a data transmission from a tag that could contain the tag's ID. When this data transmission is retransmitted, it appears to be a valid tag. Thus, the reader system cannot determine that data transmission is not authenticated [11], [12].

D. Tracking:

A primary security concern is the illicit tracking of RFID tags. Tags which are world-readable, pose a risk to both personal location privacy and corporate security. Since tag can be read from inside wallets, suitcases etc. even in places where it's not expected to items to move often it can be a smart idea to find ways to track the item. Current RFID deployments can be used to track people the tag the carry. To solve this problem, we cannot use a fixed identifier [7], [12].

III. Related Work

To resolve the security concerns rose in the previous section many protocols have been proposed in various research papers.

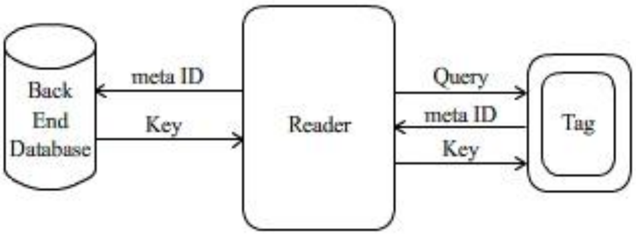

Fig. 3

In the work [4], the authors proposed a 'Hash lock Scheme'. In this scheme, the tag carries a key and a meta ID that is nothing but the hashed key. Upon request from a reader, the tag sends its stored meta ID back to the reader. Reader then forwards this meta ID to the back end database where the key of the tag has been found by looking up the database using meta ID as the search key. The reader forwards the key found from the database to the tag which hashes this key value and matches the calculated hashed value with the stored meta ID. On a successful match the tag is unlocked for further information fetch.

The drawback of this protocol is that the meta ID is still unique. A tag can still be tracked using this meta ID despite of knowing the original ID. So, "location privacy" is still under threat. Again, while transmission of the key from back end database through reader, it can easily be captured by an eavesdropper though the connection between the reader and tag has been an authenticated one. Hence, eavesdropping is still a major problem. From this, it is inferred that no 'unique' and 'static' value can ever be sent back to the reader.

To overcome this problem, a new protocol has been predicted [4] in which tag responses change with every query. To realize this, the tag sends a pair <r, h(ID, r)> where r is a random number upon request. The database searches exhaustively through its list of known IDs until it finds the one that matches h(ID,r), for the given r. Though this technique resolves the tracking problem yet increases the overhead of the database and the search complexity increases with r. This is handled by the protocol discussed by us in the next section.

III. Security Proposals

A. Mitigating Eavesdropping:

In the first part of our work, we came up with a novel idea to alleviate eavesdropping introducing meta ID concept in a new light.

Our tag contains a unique meta ID. As we cannot send the unique meta ID, we are generating a random number in the tag. This random number is fed to a down counter. The down counter counts down to zero and sends a clock pulse to a sequence generator with each down count, on receiving of which the sequence generator each time generates a new state starting from the state equivalent to the meta ID. When the down counter becomes zero, the state of sequence generator is recorded.

Tag sends a pair <r, q> where r is the random number and q is the new state generated by the sequence generator. At the reader end a reverse sequence generator is implemented through which the state equal to the original meta ID has been found.

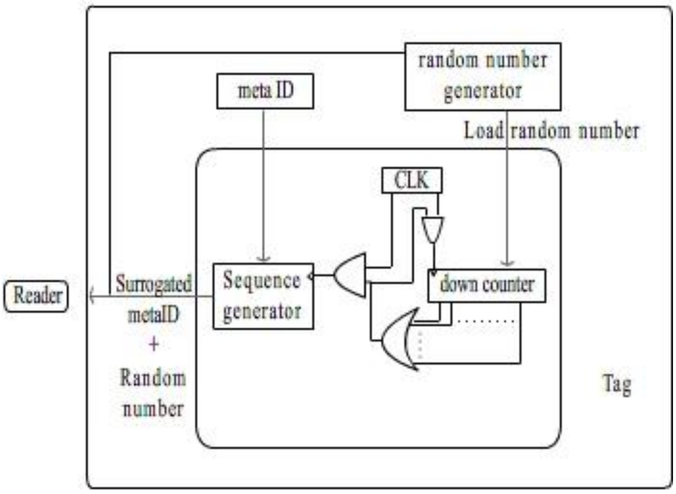

Fig. 4

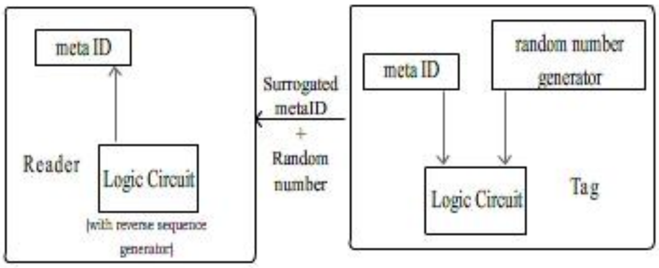

Fig. 5

B. Reader Identification:

Since the reader plays an important role in RFID system, the tag must identify its authenticated reader. An authenticated reader has the capability to modify, change, insert or delete the tag's data. As an extension to the previous section, after generating the original meta ID the system looks into the back-end database and retrieves the corresponding key. Now, before sending the key to the tag, the logic circuit effaces some of the bits from the key and sends the modified key to the tag. Which bits are to be deleted is determined by the random number r.

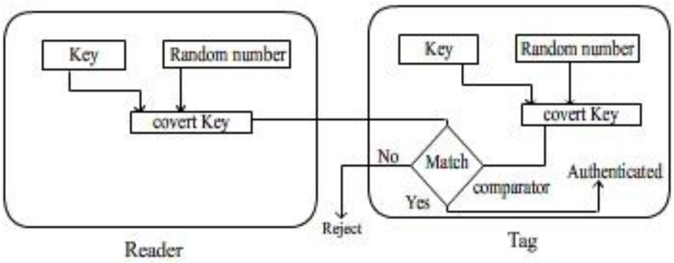

Fig. 6 Example of an image with acceptable resolution

At the tag end, the missing bits of the covert key are copied down from the original key stored in the tag. Then the stored key and the modified key are compared. On a successful match, the tag considers the reader to be valid and unlocks itself for further access of the reader. Otherwise, it rejects the query request sensing the reader to be a false one.

C. Slotted ID Read:

Up to this stage only a valid reader has been given the privilege to gain access of the next level of the tag. Still the unique ID of the tag cannot be sent openly to the reader as it can readily get skimmed and tracked by an eavesdropper. To deal with it, the ID is divided into a number of fixed length slots(l), only a part of which contains the data part. The length of the data portion (p) is determined by the formula-

$p = r \bmod l$

where, r = previously generated random number
l = the length of entire unique ID
p = length of data part in each packet

The rest of the packet of length (l-p) is padded with extra bits. Then the entire data packet is encrypted. As only the authenticated reader knows the random number, it provides an extra security to this approach. The transmission of data packets in several slots is continued until the end of the ID.

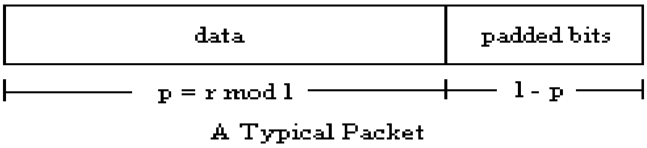

Fig. 7

D. Tag Identification:

At the reader end after receiving the each data packet, it first decrypts the data and then discards the padded bits. This method is continued for each packet and then the decrypted IDs are combined together to reform the entire unique ID. Thus, the unique ID is transmitted to the authenticated reader and at the same time it also stymied the false readers from reading it.

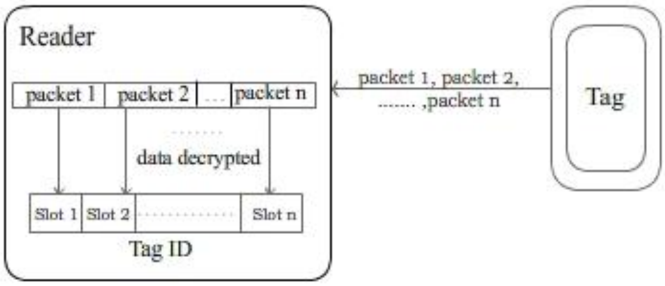

Fig. 8 Example of an image with acceptable resolution

IV. Security Analysis

In our protocol, we have provided a four step security to the ID that prevents the tag from getting cloned and reduces the risk of spoofing, eavesdropping by many folds.

Step 1:

As the <r, q> pair sent to the reader from the tag changes every time, an eavesdropper can never track a tag through its meta ID. In work [4] though this was achieved, it increased the database overhead and complexity of brute-force search algorithm. In our method, the same goal was met but the problem of work [4] has also been resolved.

Step 2:

The key retrieved from the back-end database of the reader has not directly been sent to the tag as any false reader can catch this key on its way to the tag and can prove itself to be a valid reader at any moment. Hence, the key has been modified with special method and as the same key is modified in a different manner each time, it doesn't allow a false reader or an eavesdropper to discover the key.

Step 3:

The received and modified key is reconstructed and matched with the key stored in the tag to authenticate a reader. This feature bars all readers apart from the valid one to gain further access of the tag contents.

Step 4:

The entire ID has been slotted and data part of each slot is of different length for different random number which is only known to the server and client. The last few bits of each slot are padded bits. Then the data of the entire slot is being encrypted and sent to the reader. The ID is sent in several steps and the unique ID has never been sent in its original form. This entire method allows only an authenticated reader to find the original ID.

Thus, we have beefed up the security of the ID through our protocol and provided secure tag-to-reader transactions.

V. Future Scope of Research

RFID is a wide concept; it needs both time and money along with proper research lab to conduct effective and efficient ways of its implementation. Since our whole work is based on theoretical concepts there is a room for further future research keeping in mind the cost effectiveness also. As hardware plays the pivot role in practical implementation, we can work on it for cost minimization in a best and fruitful way.

It can be that our protocol be mixed up with other research works to make it more beneficial for practical life implementation towards the goal of manufacturing low cost RFID. With the passage of time and generation new ideas along with new technology will sprung up, which will definitely make this RFID technology, a more preferable and cost effective.

We should keep in mind another thing that is the frequency of RFID. The RFID must be implemented keeping in mind the human exposure regulation which varies from countries to countries. As the radiation from RFID is not good for human exposure, RFID radiation is inadvertently causing damage to human cells, tissues on its exposure. So there is a wide space in this field also to minimize its effect on human beings. Hence there is a plethora of fields in which we can work on.

VI. Conclusion

As our work revolves around security only, we have provided a 3-way security level in our proposal. With our limited resources we had tried our best to give tag-reader identification a higher priority since both have their own importance in security analysis measurement. By combining the random variable concept for tag-reader identification we have provided an additional security.

From our perspective, the protocol can be implemented practically without any drawback. From our past knowledge we can say that either the earlier protocols were too expensive to implement or they compromise with the security.

The most important characteristic of our protocol is that at no point of time we are leaving our IDs/keys in their original form. Even if a false reader reads any information, it's of no use for that reader. That said, our proposed security definitions are just a starting point. They certainly do not capture the full spectrum of real-world needs. We had proposed important areas for further work.

References

[1] Glidas Avoine and Philippe Oechslin, "A Scalable and Provably Secure Hash-Based RFID Protocol", *The 2nd IEEE International Workshop on Pervasive Computing and Communication Security, 2005*.

[2] C. M. Roberts, Radio frequency identification, *Computers & Security vol. 25, p. 18-26,* Elsevier, 2006.

[3] Tassos Dimitriou, A Secure and Efficient RFID Protocol that could make Big Brother (partially) Obsolete, *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications,2006*.

[4] Stephen A. Weis, Sanjay E. Sharma, Ronald L. Rivest and Daniel W. Engels, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, *1st International conference on Security in Pervasive Computing(SPC),2003*.

[5] Mike Burmester, Breno de Medeiros and Rossana Motta, *Provably Secure grouping-proofs for RFID tags*.
[6] Gildas Avoine and Philippe Oechslin, *RFID Traceability: A Multilayer Problem*.
[7] Mike Burmester and Breno de Medeiros, *RFID Security: Attacks, Countermeasures and Challenges*.
[8] G.P. Hancke, *Eavesdropping Attacks on High-Frequency RFID Tokens*.
[9] Raphael C.-W. Phan, Jiang Wu , Khaled Ouafi and Douglas R. Stinson, *Privacy Analysis of Forward and Backward Untraceable RFID Authentication Schemes*.
[10] Mayla Brus´o, Konstantinos Chatzikokolakis, and Jerry den Hartog, *Formal verification of privacy for RFID systems*.
[11] Dale R. Thompson, Neeraj Chaudhry, Craig W. Thompson, *RFID Security Threat Model.*
[12] Dong-Her Shih, *Privacy and Security Aspects of RFID Tags*.