International Journal of Electrical, Electronics and Computer Engineering **3**(1): 55-61(2014) **ISSN No. (Online): 2277-2626**

On Multilayer Problems in Radio Frequency Identification : A System Approach

Santosh Kumar Yadav* and Garima Goel**
**Director (Academic & Research), J.J.T. University, (RJ) (India)*
***Research Scholar, J.J.T. University, Rajasthan (India)*

(Corresponding author Garima Goel)
(Received 05 January, 2014 Accepted 22 February, 2014)

ABSTRACT: Radio Frequency Identification systems make possible the identification of the objects in the environment with neither physical nor visual contact. Retail, rental, surveillance etc. are the domains with RFID tags have very real and promising applications. In real life applications in an environment these tags have serious implications on the privacy of the people. Sometimes the technology concept yields serious opposition and create problems. The problem occurs beyond the application layer. RFID system have three layers viz. Application layer, Communication layer and physical layer. By observing each layer we can solve privacy problems of the whole system. The generalized policy has been used in the aspect of privacy as multilayer system.

Keywords: Privacy, multilayer, collision avoidance, PUF, RFID, system model, communication protocol.

I. INTRODUCTION

As the development of technological variants and revolution, RFID systems have made possible the unique identification of the objects in any system environment without physical or visual contacts. Transponders inserted into the system objects of readers to communicate the transponders by using radio frequency of the database containing information on the tagged objects. Although this technology has a fundamental base and has been used since decades in ticketing of public transport, motorway tollgates or ski-lifts and identification of animals and plants. In early days transponders were huge in size and the RFID technology now it has become cheaper and small in size. The transponders have now increased their computation, storage and communication capacities by using reduced capacities these transponders are called tags, being their share of problems with regard to privacy issues whether to be information leakage or traceability.

RFID tags are super barcodes of the future which are based on different technology identification by RF representation as major innovation related to optical identification. Most common area of application for RFID tags is the management of stock and inventories in the open market and warehouses. As a progressive policy it can only affect suppliers like pharma products. In the third world mass marketing like India, suppliers have started using electronic tags on the palettes and packaging boxes that are delivered to it.

One obsession of customers is cutting the waiting time at tills, replacing the shop assistants with an entirely automated device : one would simply pass the contents of the trolley through a reading tunnel. This application will not see the light of day anytime soon, principally for technical reasons, but also can be cloned or rendered ineffective through various processes, which clears the way for malicious activity. Even though barcodes can equally be cloned by a simple photocopy, this type of fraud is thwarted by a human presence when the goods are scanned at the till in case of doubt, the shop assistant can verify the appropriateness of a product with the description corresponding to the barcode. Some visionaries go even further: the tags could contain information useful in the home, like washing, cooking or storing instruction. Thus maybe the washing machine that asks for confirmation before washing whites with reds or the refrigerator that discovers that a pot of "crème fraîche" stored on its shelves is no longer as fresh as its name suggests may no longer be science fiction?

Some very cheap tags, electronic microcircuits equipped with an antenna have limited computation, storage and communication capacity due to cost and size restricted.

The storage capacities of RFID tags are also extremely limited. The cheapest devices have only between 64 and 128 bits of ROM memory, which allows the unique identifier of the tag to be stored. Adding EPROM memory remains an option for more developed applications. Whilst some memory zones can be made remotely inaccessible, the tags are not tamper-resistant, unlike smartcards made for secure applications.

The communication distance between tags and readers depends on numerous parameters, in particular the communication frequency. Two principal categories of RFID systems coexist: the systems using the frequency 13.56MHz and the systems using the frequency 860-960MHz, for which the communication distance is greater. In this latter case, the information sent by the reader can in practice be received up to a hindered meters, but the information returned from the tag to the reader reaches a few meters at most. These limits, resulting from standards and regulations, do not mean that the tags cannot be read from a greater distance: non-conforming equipment could exceed these limits, for example by transgressing the laws relating to the maximum authorized power.

II. SOME PRIVACY THREATS

Falsification of the tags and their concealment are beyond the usual denial of service attacks, threats to the functionality of RFID systems. A cheap tag cannot benefit from protection mechanism like smartcards. An adversary can obtain the memory content and create a clone of the tag of the openly transmits all its data as a common application. On reducing the reading distance reduces the risks of eavesdropping, which is not a satisfactory solution. For this purpose, high gain antenna and use of non conforming power backup levels make it possible to read a tag from greater distance. The probability to neutralize the tag also prevents the correct functionality of the system (RFID). The main threats in the privacy of RFID tag carriers are: information leakage and traceability.

To disclose the information arise during the transmission of data by the tag reveals data intrinsic to the object or the environment e.g. tagged pharmacy product can reveal data about the health of the patient. The tags are not made to contain or transmit large quantities of data. In the presence of database in the system, the tag can send a simple identifier so that only a person who has access to this database which can match the identifies to the corresponding information. This is the main principle adopted by systems using barcodes. A complex problem of traceability, if the tag only transmits an identifier as an information that can be used to trace an object in time and space.

For a link that can be established between a person and the tags are carried out, the tracing of objects can become the tracing of a person. Attacker wants to trace a tag either deterministically or probabilistically starting from active or passive attack.

III. PHYSICAL UNCLONEABLE FUNCTIONS

A ‘Physical Uncloneable Function’ (PUF) is a function that is realized by a physical system, such that the function is easy to evaluate but the physical system is hard to characterize [2]. PUFs have been proposed as a cost-effective way to produce uncloneable tokens for identification [4]. The identification information is contained in a cheap, randomly produced (i.e. consisting of many random components), highly complicated piece of material. The secret identifiers are read out by performing measurements on the physical system and performing some additional computations on the measurement results. The advantage of PUFs over electronic identifiers lies in the following facts: (1) Since PUFs consist of many random components, it is very hard to make a clone, either a physical copy or a computer model, (2) PUFs provide inherent tamper-evidence due to their sensitivity to change in measurement conditions, (3) Data erasure is automatic if a PUF is damaged by a probe, since the output strongly depends on many random components in the PUF. Additionally one can extract cryptographic keys from a PUF. This makes PUFs attractive for Digital Rights Management (DRM) systems.

Optical PUFs are well suited for identification, authentication and key generation. The goal of an identification protocol is to check whether a specific PUF is present at the reader. The goal of an authentication protocol is to ensure that received message originate from the stated sender. For authentication it is therefore the objective to extract the same cryptographic key from the PUF as the one that is stored at the Verifier’s database during enrollment, while for identification it is sufficient if the response is close to the enrolled response.

In order to use PUFs for above mentioned purposes they are embedded into objects such as smartcards, creditcards, the optics of a security camera, etc., preferably in an inseparable way, meaning that the PUF gets damaged if
an attacker attempts uniquely identifiable and uncloneable. Secrets keys can be derived from a PUF’s output [4] by means of protocols similar to those developed in the context of biometrics [5].

IV. NECESSARY PROTOCOLS

The device and the Verifier need to exchange secret messages, a secure authenticated channel is set up between them, using a session key based on the PUF response. We present the following protocols.

A. Identification Protocol

- User: Puts his card with PUF in the reader and claims its ID.
- Verifier: Randomly chooses a challenge *C* form his CRP database and sends it to the User.
- Reader: Challenges the PUF with the Challenge *C*, measures the Response *R* and computes an identifier S'. S' is sent back to the Verifier.
- Verifier: Checks whether S' equals the identifier *S* stored in his database during enrollment. Then he removes the pair (*C*, *S*) from his database and never uses it again.

We note that the security of this protocol relies on the fact that an attacker who has seen (C_1, S_1) cannot predict the identifier S_2 corresponding to the challenge C_2, and on the fact that the PUF supports a large number of CRPs.

B. Authentication Protocol

- User: Puts his card with PUF in the reader and claims its ID.
- Verifier: Randomly chooses a challenge *C* form his CRP database and sends it to the User, together with a random nonce *m*.
- Reader: Challenges the PUF with the Challenge *C*, measures the Response *R* and computes a key S'. $M_{S'}(m)$ is sent to the Verifier, where $M_{S'}(m)$ denotes a MAC on *m*, using the key S'.
- Verifier: Computes $M_S(m)$ with the key *S* stored in his database and compares it with $M_{S'}(m)$. If they are equal, then $S = S'$ with very high probability. The key *S* is then used to MAC and/or encrypt all further messages.

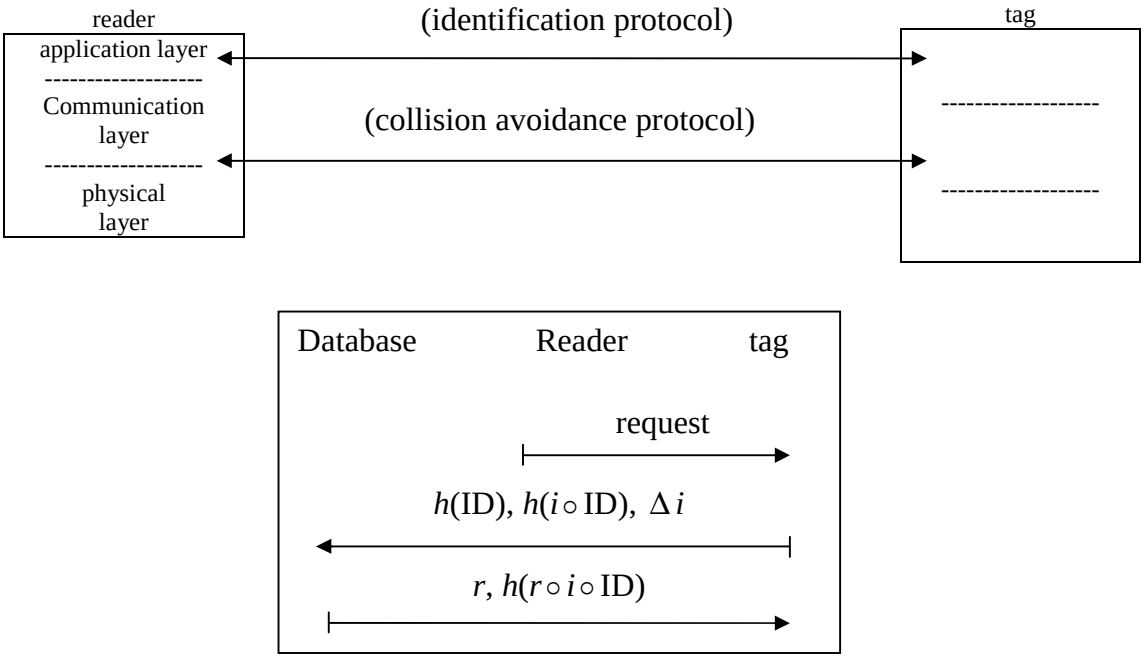
The security of this scheme depends on the fact that (when the key S is unknown) the MAC $M_S(m)$ is unpredictable given that the attacker has seen the MAC on a message $m_1 \neq m$.

V. TRACEABILITY ↔ LAYERS

Confidentially, integrity and authentication are the basic concepts that are considered in cryptography. These three concepts are analyzed by a model of the adversary in the entities and the communication channels in order to compromise the above three concepts of cryptography. It is a theoretic concept which is usually defined temperproofness of the entities or timeliness of the channels without considering the absolute nature of the physical architecture. (refer fig 1 for base model)

A. The Application Layer

This layer handles the information defined by the user. This is the information about the tagged object or more probability an identifier allowing the reader to extract the corresponding information from the database. The identifier can be protected if an application protocol transforms the data before it is transmitted or deliver the information only if certain conditions are fulfilled. A protocol generated by Henrici and Muüller. Accordingly after the personalization phase, the tag contains its current identifier (ID), the current session number *i* and the last successful session number i^*. When the system is launched , the database contains a list of entries, one for each tag it manages. Each entry contains the same data as is stored in the tag, augmented by a hash value of ID, *h*(ID), which constitutes the database primary key and other additional data. ID and *i* are set up with random values and i^* equals *i*. The identification process is as follows



2 Herici and Müller protocol.

1. The reader sends a request to the tag.
2.The tag increases its current session number by one. It then sends back h(ID), $h(i \circ \text{ID})$ and $\Delta i := i - i^*$ to the reader which forwards the values to the database. Here ∘ is a "suitable conjunction function"; "A simple exclusive or function is adequate for the purpose". h(ID) allows the database to recover the identity of the tag in its data; $h(i \circ \text{ID})$ aims at thwarting replay attacks and Δi is used by the database to recover i and therefore to compute $h(i \circ \text{ID})$.
3. The database checks the validity of these values according to its recorded data. If all is fine, it sends a random number r and the value $h(r \circ i \circ \text{ID})$ to the tag, through the reader.
4. Since the tag knows i and ID and receives r, it can check whether or not $h(r \circ i \circ \text{ID})$ is correct. If this is case, the tag calculates its new identifier $\text{ID}' := r \circ \text{ID}$ and $i^* := i$, which is used in the next identification. Otherwise it does not calculate ID'.

B. The Communication Layer

This layer defines the way in which the readers and tags can communicate each other. This layer consists of collision avoidance protocols as well as an identifier makes it possible to single out a specific tag for communication with a reader (not like application layer). The commonly used protocols in this layer are as under.

Singulation protocols are to avoid collision and information loss. This arises in RIFD systems because when a reader sends a request, all the tags in its field reply simultaneously, causing collisions. The required rules are known as the *collision avoidance* protocol. The tags' computational power is very limited and they are unable to communicate with each other. therefore, the readers must deal with the collision avoidance themselves, without the help of tags. Usually, they consist of querying the tags until all identifiers are obtained. The reader performs the *singulation* of the tags because it can then request them selectively, without collision, by indicating the identifier of the queried tag in its request.

Deterministic protocols rely on the fact that each tag has a unique identifier. It we want the singulation process to succeed, the identifiers must stay unchanged until the end of the process. In the current tags, the identifiers are set by the manufacturer of the tag and written in the tag's ROM. In the usual RFID systems, there is no exchange after the singulation because the reader has obtained the expected information, i.e., the identifiers of the tags which are in its field. Below, we use *singulation identifier* to denote such an identifier, or more simply *identifier* where there is no ambiguity with the identifier of the application layer.

Probabilistic protocols are based on a time-division multiple access protocol, called *Aloha*. We describe one of the variants of Aloha, namely the slotted Aloha. In the slotted Aloha, the access to the communication channel is split into time slots. In general, the number of slots is chosen randomly by the reader which informs the tags that they will have *n* slots to answer to its singulation request. Each tag randomly chooses one slot among the *n* and responds to the reader when its slot arrives. If *n* is not sufficiently largfe with regard to the number of tags which are present, then some collisions occur. In order to recover the missing information, the reader interrogates the tags one more time. It can mute the tags which have not brought out collisions (*switched-off* technique) by indidicating their identifiers or the time slots during which they transmitted. Also, according to the number of collisions, it can choose a more appropriate *n*.

The singulation identifier cannot be changed during a session, the idea, to avoid traceability, is to use an identifier which is different for each session. The fact that the tag can be tracked during a session is not really a problem due to the shortness of such a session. The notion of singulation session already informally exists because the readers usually send a signal at the beginning and end of a singulatin. Unfortunately, there is no reason to trust the readersto correctly accomplish this task. A malicious reader can voluntarily keep a session open to track the tag thanks to the unchanged identifier. This attack cannot be avoided when the signals come from the reader and not from the tag itself.

To illustrate our point, we can analyse the collsion avoidance protocol proposed by Philips for tis tag ICode1 Label IC [7] usin the 13.56MHz frequency. It contains a 64 bit identifier of which only 32 are used for the singulation process, denoted by $b_1 \ldots b_{32}$. Although the tag does not have a PRNG, the implemented collision avoidance protocol is probablisitic. The choice of the time slot depends on the identifier of the tag and data sent by the reader. When the reader queires a tag, it sends a request containing: the number of slots *n* which the tags can use, where $n \in \{2^0, 2^1, \ldots, 2^8\}$, and a value $h \in 0,\ldots, 25$ called *hash value*. The section of the time slot s_i is done as follows:

$$s_i := CRC8(b_{h+1} \ldots b_{h+8} \oplus prev) \oplus n$$

where CRC8 is a *Cyclic Redundancy Check* with generator polynomial $x^8 + x^4 + x^3 + x^2 + 1$ and where *prev* is the output of the previous CRC8, intialised with 0*x*01when the tag enters the field of a reade. Hence, an adversary can easily track a tag according to the slot chosen by the tag, if he always sends the same values *h* and *n*.

An adversary sends to his (isolated) targeted tag a request with the number of slots *n* and the hash value *h*. The tag responds during slot s_{target}. When he meets a set of *m* tags, the adversary wants to know if his target is here. In order to do this, he sends a singulation request containing the same *n* and *h*. If no tag responds during s_{target} then the target is not included in the set of tags. However, the conditional probability that the tag is in the set given that at least one tag answers during slot s_{target} is

$$P(n, m, p) = \frac{p}{p + (1-p)\left(1 - \left(\frac{n-1}{n}\right)^m\right)},$$

C. Physical Layer

This layer defines the physical air interface i.e., the frequency, modulation of transmission, data encoding, timing etc. The physical signals exchanged between a tag and a reader can allow an adversary to recognize a tag or a set of tags even in the information exchanged can not be understood. All efforts to prevent traceability in the higher layers may be rendered useless if no care is taken at the physical layer.

To reduce the threats of traceability due to characteristic groups of tags it is thus of paramount importance to reduce the diversity of the standards used in the market. Note that even if it is possible to agree on a single standard to use when RFID tags become popular, there will be times when a standard for a new generaion of tags will be introduced. During the period of transition it will be possible to trace people due to characteristic mixes of old and new tags.

Preventing traceability through radio fingerprinting seems quite difficult. There is no benefit for the manufacturers to produce tags that use exactly the same technology, producing the same radio fingerprint. Much more likely, manufactures will experiment with different technologies in order to produce tags that have either better performance, price or size.

VI. COMMUNICATION WAVE GUIDE (MATHEMATICAL MODEL)

We compute the number of incoming and outgoing mode N_{mod}. The complex amplitude of

the electric field on communication surface can be represented as

$$E(r) = \int_{|q|\le k} \frac{d^2q}{(2\pi)^2} \overline{E}(q) e^{iq.r};$$

$$\tilde{E}(q) = \int_{|x|,|y|\le W/2} d^2r\ E(r) e^{-iq.r}$$

where $r = (x, y)$ denotes the position and $q = (q_x, q_y)$ the lateral wave vector. A mode is propagating if the longitudinal (z) component of the wave, $q_z = \sqrt{k^2 - q^2}$, is real (where $k = 2\pi/\lambda$). Hence the integration domain is a circle in q-space with radius k. Note that both $E(r)$ and $\tilde{E}(q)$ are band-limited functions. Applying the Shannon-Whittaker sampling theorem [7] to the expression for $\tilde{E}(q)$ in [1] , it follows that $\tilde{E}(q)$ can be characterized by discrete samples,

$$\tilde{E}(q) = \sum_{ax,ay=-\infty}^{\infty} \tilde{E}\left(a_x \frac{2\pi}{W}, a_y \frac{2\pi}{W}\right) \frac{\sin(q_x W/2 - a_x\pi)}{q_x W/2 - a_x\pi} \frac{\sin(q_y W/2 - a_y\pi)}{q_y W/2 - a_y\pi}$$

Next, we use the fact that the electric field is band-limited in q-space as well. The integers a_x, a_y have to satisfy $(a_x^2 + a_y^2)(2\pi/W)^2 \le k^2$. The number of modes is therefore finite and is given by the number of pairs (a_x, a_y) satisfying the momentum constraint $|q| \le k$. Denoting the transverse modes as q_a, we have

$$q_a = \frac{2\pi}{W}(a_x, a_y);\ N_{\text{mod}} = \#\{(a_x, a_y)\ with\ |q_a| \le k\} = \frac{\pi A}{\lambda^2}$$

The integers a_x, a_y lie in the range $(-W/\lambda, W/\lambda)$. The angular distance between outgoing modes corresponds to the correlation length present in the speckle pattern as derived by [8].the scattering process can be represented as a complex random matrix S, whose elements map incoming states to outgoing states,

$$\tilde{E}_a^{out} = \sum_{b=1}^{N_{\text{mod}}} S_{ab}\ \tilde{E}_b^{in}$$

We take the distribution function of S to be symmetric in all modes. We introduce $T_{ab} = |S_{ab}|^2$, the transmission coefficient from mode b to mode a, which specifies how much light *intensity* is scattered. Given a basic challenge, consisting of a single incoming mode b, a speckle pattern corresponds to an $N_{\text{mod}-}$ component vector v, namely the b'th column of the T-matirx,

$$v_a = T_{ab}, b \text{ fixed.}$$

VII. CONCLUSION AND FUTURE TRENDS

In RIFD systems only a little concerned with classical cryptographical models for the practical aspects on traceability in general practice. RFID in based on three basic concepts of cryptography, but, it is considered with respect to communication architecture of cryptographic model. RFID can create fully privacy to ensure three layers of communication model for which all possible threats can be detected easily. It is (I) cheap, robust and market friendly. RFID has strong protocol structure and can be implemented in a well organized manner. The mathematical modeling can be used in simple programming structure in a basic language.

REFERENCES

[1]. Gildas avoire and Philippe Oechslin, *RFID Traceability: A Multilayer Problem* LNCS3570, pp. 125-140, 2005.

[2]. B. Gassend et al., *Controlled Physical Random Function*, Proc. 18th Annual Computer Security Applications Conf., Dec. 2002.

[3]. B. Gassend et al., *Silicon Physical Unknown Functions*, Proc. 9th ACM Conf. on Computer and Communication Security, Nov. 2002. (II)

[4]. D. Henrici and P. Müller. Hash-based enhancement of location privacy for radio frequency identification devices using varying identifiers. *Workshop on Pervasive Computing and Communications Security – PerSec 2004*, pp. 149-153, IEEE, 2004.

[5]. A. Juels, "yoking-proofs" for RFID tags. *Workshop on Pervasive Computing and Communications Security – PerSec 2004*, pp. 138-143, IEEE, 2004.

[6]. A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. *Conference on Computer and Communications Security – ACM CCS*, pp. 103-111, ACM, 2003.

[7]. P. Tuyls, B. Skoric, *Secret Key Generation from Classical Physics*, Proceedings of the Hardware Technology Drivers for Ambient Intelligence Symposium, Philips Research Book Series, Kluwer, 2005.

[8]. J. P. Linnartz, P. Tuyls, *New Shielding Functions to enhance Privacy and Prevent Misuse of Biometric Templates*, Proc. 4th International Conference on Audio and Video based Biometric Person Authentication, LNCS2688, Guildford UK, June 9-11, 2003.

[9]. ISO/IEC 7498-1:1994. Information technology – open systems interconnection basic reference model: The basic model. http://iso,org, November 1994.

[10]. J. Saito, J. –C. Ryou, and K. Sakurai. Enhancing privacy of universal re-encryption scheme for RFID tags. *Embedded and Ubiquitous Computing – EUC 2004*, LNCS 3207, pp. 879-890, Springer, 2004.

[11]. J. Toonstra and W. Kinsner. Transient analysis and genetic algorithms for classification. *IEEE WESCANEX 95. Communications, Power and Computing*, volume **2**, pp. 432-437, IEEE, 1995.

[12]. S. Weis. Security and privacy in radio-frequency identification devices (master thesis), May 2003.

[13]. E. Verbitskiy, P. Tuyls, D. Denteneer, J. P. Linnartz, *Reliable Biometric Authentication with Privacy Protection*, Proc. of the 24th Symposium on Information Theory in the Benelux.

[14]. T. M. Cover, J. A. Thomas, *Elements of Information Theory*, Wiley ans Sons, New York, 1991.

[15]. K. Petersen, *Ergodic Theory*, Cambridge University Press, 2000.

[16]. Yadav Santosh Kumar, *Some Problems in Symmetric and Asymmetric Cryptography*, LAP Lambart Publication, Germany, 2013.