Diffusing RFID-Sensor Networks and Security Threats

TAI-HOON KIM
Multimedia Engineering Department,
Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon,
Korea
taihoonn@hnu.kr

Abstract

To uniquely identify physical objects, Radio Frequency Identification (RFID) systems are used with its limitless possibilities and low cost. RFID is a method of remotely storing and retrieving data using devices called RFID tags. An RFID tag is a small object, such as an adhesive sticker, that can be attached to or incorporated into a product. But with this common scenario involving numerous tags and present in the interrogation zone of a single reader at the same time. RFID is prone to security threat as well, which is the main focus of this paper. In this paper we present an anti-collision protocol existing and applied in the RFID dilemma, sited vulnerabilities and suggested general security solutions.

Keywords: RFID, Security, Threats

1. Introduction

RFID systems can be used just about anywhere, from clothing tags to missiles to pet tags to food -- anywhere that a unique identification system is needed. The tag can carry information as simple as a pet owners name and address or the cleaning instruction on a sweater to as complex as instructions on how to assemble a car. Some auto manufacturers use RFID systems to move cars through an assembly line. At each successive stage of production, the RFID tag tells the computers what the next step of automated assembly is. [1]

Radio frequency identification (RFID) systems are gaining much attention in many, manufacturing companies, industries, etc. These systems consist of networked electromagnetic readers and tags, where the readers try to identify the tags as quickly as possible via wireless communications. However, since the readers or the tags communicate over the shared wireless channel, the collision problem occurs in signal transmission of the readers or the tags, which hardly leads to fast identification. Thus, it is a key issue to develop an efficient anti-collision protocol reducing collisions so as to search all the tags in the interrogation zone.

2. RFID (Radio Frequency Identification)

2.1 RFID System Components

RFID systems are made up of three main components, which we briefly describe in the following: the transponder or RFID tag, the transceiver or RFID reader, and the back-end database.

1. Transponder or RFID Tag In an RFID system, each object will be labeled with a tag. Each tag contains a microchip with some computation and storage capabilities, and a coupling element, such as an antenna coil for communication. Tags can be classified according to two main criteria:

   - The type of memory: read-only, write-once read-many, or fully rewritable.

- The source of power: active, semi-passive, and passive.

2. Transceiver or RFID Reader RFID readers are generally composed of an RF module, a control unit, and a coupling element to interrogate electronic tags via RF communication. Readers may have better internal storage and processing capabilities, and frequently connect to back-end databases. Complex computations, such as all kind of cryptographic operations, may be carried out by RFID readers, as they usually do not have more limitations than those found in modern handheld devices or PDAs.
3. Back-end Database
   The information provided by tags is usually an index to a back-end database (pointers, randomized IDs, etc.). This limits the information stored in tags to only a few bits, typically 96, which is a sensible choice due to tag severe limitations in processing and storing. It is generally assumed that the connection between readers and back-end databases is secure, because processing and storing constraints are not so tight in readers, and common solutions such as SSL/TLS can be used.

2.2 RFID System Interface

In this section, we focus exclusively on passive RFID tags, since we consider that these will be the first to be massively deployed and form part of our daily lives. Additionally, these low-cost RFID systems are very limited on resources, which forces some interesting trade-offs in their designs.

1. Transceiver/Transponder Coupling Communication Passive RFID tags obtain their operating power by harvesting energy from the electromagnetic field of the reader communication signal. Two main possibilities exist here: near field (d < 1 2¼f) and far field (d > 1 2¼f) [2]. The signal sent from readers to tags must be used simultaneously to transmit both information and energy. However, readers normally operate in Industrial Scientific-Medical (ISM) bands, so there are restrictions in the bandwidth and in the transmitted power. Tags, on the other hand, are not under these limitations.

2. Data Coding The exchange of data between the reader and the tag, and vice versa, must be performed efficiently; so both coding and modulation are used. The coding/modulation is defined according to the existing limitations in the backward and the forward channel. Readers will be able to transmit greater power, but will have bandwidth limitations. Tags, which are passive, will not have bandwidth limitations. As a coding mechanism, level codes (Non-Return-to-Zero, NRZ; and Return to Zero, RZ) or transition codes (Pulse Pause Modulation, PPM; Pulse Weight Modulation, PWM; and Manchester) are mostly used. These coding techniques are depicted in Table 1.

Table 1. Coding Technique

Channel	Usual Coding
Forward Channel	Manchester or NRZ
Backward Channel	PPM or PWM

3. Modulation

The modulation scheme determines how the bit stream is transmitted between readers and tags, and vice versa. Three possible solutions exist: Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK) and Phase Shift Keying (PSK). The choice of a modulation type is based on

power consumption, reliability, and bandwidth requirements.

4. Tag Anti-collision
Collisions in RFID systems happen when multiple tags simultaneously answer to a reader signal. Methods used to solve this kind of problems, allowing reliable communication between readers and tags, are referred to as anti-collision methods. The anti-collision algorithms used in RFID systems are quite similar to those applied in networks, but they take into account that RFID tags are generally more limited than the average network device. Two approaches are used: probabilistic or deterministic. However, in practice, many solutions are a combination of both.

5. Reader Anti-collision
In this case, several readers interrogate the same tag at the same time. This is known in the bibliography as the Reader Collision Problem. One possible solution to this problem consists of allocating frequencies over time to a set of readers by either a distributed or a centralized approach.

6. Frequencies and Regulations
Most RFID systems operate in ISM bands [15]. ISM Bands are designated by the International Union of Telecommunications and are freely available to be used by low-power, short-range systems. The most commonly used ISM frequencies for RFID systems are 13.56 MHz and 902-928 MHz (only in the US). Each band has its own radiation power and bandwidth regulations.

3. Related Work

In this section, we discuss briefly about the existing medium access schemes for RFID system. EPC Class 1 Generation 2 Standard [4] uses spectral planning (FDMA). It separates the reader transmissions and the tag transmissions spectrally such that tags collide with tags but not with readers and readers collide with readers but not with tags. Such separation solves the reader to reader interference since the reader transmissions and tag transmissions are on separate frequency channels. However, the tags do not have frequency selectivity. When two readers using separate frequency communicate with the tags simultaneously, the tag will not be able to tune to a particular frequency and hence it will lead to collision.
The Color wave [1] is the representative of algorithms that use a distributed system. The readers divide the time into frames and communicate with tags during a timeslot in a frame. If there is collision in the network, node selects a new timeslot and sends a kick to its neighbors which have the same color. In the Enhanced Colorwave [5], the reader synchronizes the frame size with that of the neighboring reader when it increases its frame size. However, they both assume that readers can detect collisions in the RFID network. Actually, it may not be practical for a reader alone to detect the collision.
The HiQ [2] is a hierarchical, online learning algorithm that finds dynamic solutions to the reader collision problem in RFID system by learning the collision patterns of the readers and by effectively assigning frequencies over time to the readers. However, it may take long time to learn the collision pattern if the network size is large. In addition, HiQ assumes collision detection for readers which are not in sensing range of each other. Actually not all collision might be detected leading to incorrect operation of the protocol.
The Pulse [3] divides the channel to the control channel and data communicating channel. Control channel is used to communicate between readers to negotiate reading sequence. The data communication channel is used for reading tags. It works by LBT scheme. Before reading tags, a reader transfers a beacon message to its neighbors through the control channel. Even it can solve the hidden terminal problem, it may cause unfairness problem. Furthermore, it requires RFID reader has an additional control channel. The enhanced Pulse [6] uses slot occupied probability (SOP) to estimate if there is other reader which are supposed to communicate with tags during the same time slot. Like Pulse, it assumes there are two channels. The Slotted-LBT [7] divides the air time into several time slots and operates by the LBT in each slot. It requires synchronization among readers. This is achieved by frame

synchronization signal and slot synchronization signal. It also can distinguish and control each channel according to the requirement specifications of various applications. However, maintaining synchronization will require extra management overhead. Some other related studies are in [41,42].

4. Existing Anti-Collision Protocols

A. System Design of RFID-Sensor Integrated Networks Technological convergence is one of hot issues due to the limitation of technologies, functions and markets [8]. There are some works about how to integrate RFID and sensor networks which collect environment and location information. In [9], the author proposed a sensor and RFID integration networks called SARIF for environment-sensitive object tracking and management. The authors work is based on an RFID-Sensor integrated network. In this network, the module node is constituted by three parts which are RFID reader (960MHz), micro-controller and RF transceiver (2.4GHz). This RFID-Sensor node also can be called node for simple. The RFID reader is able to communicate with tags within their respective interrogation zone which attached on the objects storing the information of them. The sensor can gather the environment information such as temperature, humidity and its location information. Integrated nodes can be fixed or moving depending on the application requirement. By using this node, system can provide both remote monitoring and location tracking services such as finding the inventory and checking the temperature of the storehouse and location of the products. Figure 1 shows the system architecture of the RFID-Sensor integrated network. Service provider publishes services through integrated server. User client sends their application request to the server. Gateway is the connection between core network (Internet) and RFID-Sensor integrated network. It organizes the nodes hierarchically. Nodes are divided into clusters. Each cluster has a cluster header (CH). Nodes send information to CHs. CHs transmit information to gateway. Then gateway forwards it to the server. At last, the server delivers the results to the user client. In this system, passive tags are used because of the low cost. Reference nodes equipped by GPS devices are used for localization. There are four layers in the network: gateway, CHs, RFID-Sensor nodes and tags. RFID reader communicates with the tags using 960MHz frequency while nodes communicate to CH and each other using 2.4GHz frequency. This cluster architecture facilitates the distribution of control over the network and achieves spatial reuse of network resources.

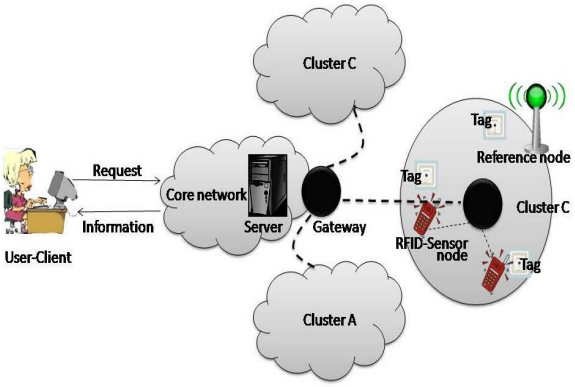

Figure 1 System Architecture of RFID-Sensor Networks

Next figure indicates the communication tree of the system. There are four layers: gateway, cluster headers, RFID-Sensor nodes and tags. RFID readers communicate with the tags using 960MHz frequency. RFID-Sensor nodes communicate to cluster headers using 2.4GHz frequency.

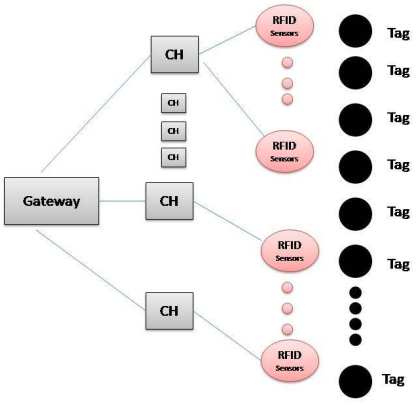

Figure 2 system Communication tree of RFID-Sensor Networks

B. Reader Collision Problem Each reader of RFID reader network has a limited interrogation zone. Only within this range can the tag be recognized. When multi-readers are deployed in a limited area, two or more readers' interrogation zone can be overlapped. If called reader ollision problem. The reader collision can be divided into two categories. One is reader-to-reader interference. It occurs when a reader transmits a signal that interferes with the operation of another reader, thus preventing the second reader from communicating with tags in its interrogation zone. Figure 3 shows the reader-to-reader interference. In figure 3, if R1 and R2 communicate with tags at the same time using the same frequency, the collision will occur. The second type of reader collision, called reader-to-tag collision, may occur when a tag is in the interrogation zone of multiple readers and more than one reader simultaneously.

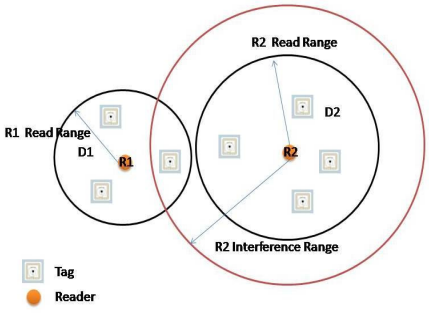

Figure 3 The reader-to-reader interference

Figure 4 indicates the reader-to-tag interference. Tag T is in the interrogation zones of both R1 and R2. If R1 and R2 send read-tag command at the same time, their signals will collide
with each other at T.

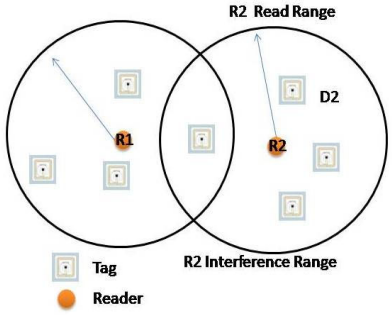

Figure 4 Reader-to-tag interfaces

6. RFID Standards

RFID systems do not lack standards. Those standards typically describe the physical and the link layers, covering aspects such as the air interface, anti-collision mechanisms, communication protocols and security functions. Never the less, not everything is well covered, and there is a certain absence of standardization in testing methods and application data (notably in protocols and application programming interfaces).

6.1 Contactless Integrated Circuit Cards

ISO 7810 defines a special type of identification cards without contact. According to the communication range, three types of cards can be distinguished:

- Close-coupled cards (ISO 10536). These are cards that operate at a very short distance of the reader (< 1 centimeter).

-Proximity cards (ISO 14443). These are cards that operate at an approximated distance of 10 centimeters of the reader. They can be considered as a high-end RFID transponder since they have a microprocessor.

- Vicinity cards (ISO 15693). These are cards that operate at distances greater than one meter. On the contrary, for the previous cards (ISO 14443), it usually incorporate only inexpensive machines of states, instead of microprocessors.

6.2 RFID in Animals

ISO 11784, ISO 11785, and ISO 14223 standardize tags for animal identification in the frequency band below 135 KHz. Initially, standards define an identifier of 64 bits. In ISO 14223, greater blocks for reading and writing, as well as blocks of protected writing, are allowed. There are hardly any divergences between the

communication protocols defined in ISO 14223 and ISO 18000-2.

6.3 Item Management

ISO 18000 defines the air interface, collision detection mechanisms, and the communication protocol for item tags in different frequency bands.

- Part 1 describes the reference architecture.
- Parts 2-7 specify the system in different frequency bands (<135KHz, 13.56 MHz, 2.45 GHz, 5.8 GHz, 900 MHz, and 433 MHz).

6.4 Near-Field Communication (NFC)

1. NFCIP-1

NFC is designed for interactions between tags and electronic devices in close proximity (< 10 cm). The standards ETSI TS 102.190, ISO 18092, and ECMA 340 identically define the Near Field Communications Interface and Protocol-1 (NFCIP-1).

These protocols describe the air interface, initialization, collision avoidance, a frame format, and a block-oriented data-exchange protocol with error handling. Additionally, they describe two different communication modes: active and passive.

2. NFCIP-2

The Near Field Communication Interface and Protocol-2 (NFCIP-2) specifies the communication mode selection mechanism (ECMA 352). NFCIP-2 compliant devices can enter in three different communication modes: NFCIP-1, ISO 14443, and ISO 15693. All these modes operate at 13.56 MHz and are designed not to disturb other RF fields at the same frequency.

6.5 Electronic Product Code (EPC)

The Auto-ID (Automatic Identification) Center was created in October 1999 at the MIT Department of Mechanical Engineering, by a number of leading figures. At the beginning, EPC was developed by the Auto-ID Center. The Auto-ID Center officially closed the 26th October, 2003. The center had completed its work and transferred his technology to EPC global [9]. EPC global is a joint venture between EAN International and the Uniform Code Council (UCC). The so-called EPC network is composed of five functional elements:

- The Electronic Product Code is a 96-bit number with 4 distinct fields: identifying the EPC version number, domains, object classes, and individual instances.

- An Identification System which consists of RFID tags and readers. Tags can be of three different kinds (Class 0, 1, and 2). The Auto-ID Center published a protocol specification for Class 1 tags in the HF band (compatible with ISO 15693 and ISO 18000-3), and Class 0 and 1 tags in the UHF band.

- The Savant Middleware offers processing modules or services to reduce load and network traffic within the back-end systems.

- The Object Naming Service (ONS) is a network service similar to the Domain Name Service (DNS), which is a technology capable of handling the volumes of data expected in an EPC RFID system.

7. Risks and Threats

Although RFID systems may emerge as one of the most pervasive computing technologies in history, there are still a vast number of problems that need to be solved before their massive deployment. One of the fundamental issues still to be addressed is privacy. Products labeled with tags reveal sensitive information when queried by readers, and they do it indiscriminately. A problem closely related to privacy is tracking, or violations of location privacy. This is possible because the answers provided by tags are usually predictable: in fact, most of the times, tags provide always the same identifier, which will allow a third party to easily establish an association between a given tag and its holder or owner. Even in the case in which tags try not to reveal any kind of valuable information that could be used to identify themselves or their holder,

there are many situations where, by using an assembly of tags (constellation), this tracking will still be possible.
Although the two aforementioned problems are the most important security questions that arise from RFID technology, there are some others worth to mention:

1. Physical Attacks
In order to mount these attacks, it is necessary to manipulate tags physically, generally in a laboratory. Some examples of physical attacks are probe attacks, material removal through shaped charges or water etching, radiation imprinting, circuit disruption, and clock flitching, among others. RFID tags offer little or none resilience against these attacks.

2. Denial of Service (DoS)
A common example of this type of attack in RFID systems is the signal jamming of RF channels.

3. Counterfeiting
There are attacks that consist in modifying the identity of an item, generally by means of tag manipulation.

4. Spoofing
Is when an attacker is able to successfully impersonate a legitimate tag like in a man-in-the-middle attack.

5. Eavesdropping
In this type of attacks, unintended recipients are able to intercept and read messages.

6. Traffic analysis
It describes the process of intercepting and examining messages in order to extract information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, the more information can be inferred from the traffic.

8. Proposed Solution

There are lots of solutions similarly as sited in [32] Yet, in this section we present the proposed solution to solve the security problems and threats associated with the use of RFID systems. Our objective is not to give a detailed explanation of each solution, but to provide the reader with the fundamental principles and a critical review of every proposal, as well as the bibliography to be checked in case someone wishes to deepen on some aspects of this subject.

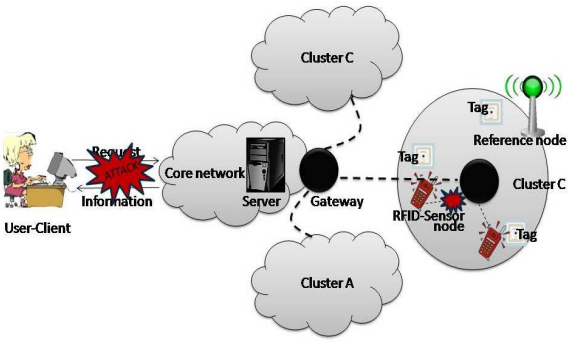

Figure 5 Security Threat for RFID-Sensor Network Anti-Collision Protocol

8.1 Lightweight Cryptographic approach

Based on security protocols MAC(Message Authentication Protocol) are among the first solutions discussed in the literature for securing low-cost RFID applications. In [33], for example, Takaragi et al. present a solution based on CMOS technology that requires less than four thousand gates to generate MACs using 128 bit identifiers stored permanently in tags at manufacturing time. Each identifier relies on an initial authentication code concatenated with manufacturing chip data. The result of this concatenation is posterior hashed with a given secret to derive a final MAC. This MAC is communicated from manufacturers to clients and shared by readers and tags. The main benefit of the approach is that it increases the technical difficulties of performing attacks like eavesdropping and rogue scanning.
However, the use of static identifiers embedded in tags at manufacturing time does not solve the tracking threat. Moreover, brute force attacks can eventually reveal the secrets shared between readers and tags. The discovery of secrets could lead to counterfeit tags. An enhanced solution relies on the use of hash-lock schemes for implementing access controls. In [35],Weis et al. propose a way to prevent unauthorized readers

from reading tag contents. A secret is sent by authorized readers to tags using a trusted environment.
Tags, equipped with an internal hash function, perform a hash on this secret and store it within their internal memory. Then, tags enter into a locked state in which they answer to any possible query with the computed hash. Weis et al. also describe proper ways of unlocking tags, if such an action is needed by authorized readers (i.e., to temporarily release private data). Regarding privacy threats, Ohkubo et al. propose in [49] the use of hash chains for the implementation of on-tag security mechanisms with evolving RFID identities. Avoine and Oechslin discuss in [2] some limitations of the approach. They propose an enhanced hash-based RFID protocol to address both authentication and privacy by using timestamps. Similarly, Henrici and Müller discuss in [25] some weaknesses in the hash-lock scheme presented in [35] and propose a new hash-based scheme intended to enhance privacy and authentication. Several other improvements and hash-based protocols, most of them inspired on lightweight cryptography research for devices with higher hardware capabilities such as smart cards, can be found in [36].
Similarly, a study of Data Transmission Encryption and Decryption Algorithm in Network Security presented in [40] is comparable to the mentioned cryptographic approach.

8.2 Kill Command
This solution was proposed by the Auto-ID Center [5] and EPC global. In this scheme, each tag has a unique password, for example of 24 bits, which is programmed at the time of manufacture. Upon receiving the correct password, the tag will deactivate forever.

8.3 The Faraday Cage Approach
Another way of protecting the privacy of objects labeled with RFID tags is by isolating them from any kind of electromagnetic waves. This can be made using what is known as a Faraday Cage (FC), a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies). There are currently a number of companies that sell this type of solution [24].

8.4 The Active Jamming Approach
Another way of obtaining isolation from electromagnetic waves, and an alternative to the FC approach, is by disturbing the radio channel, a method which is known as active jamming of RF signals. This disturbance may be done with a device that actively broadcasts radio signals, so as to completely disrupt the radio channel, thus preventing the normal operation of RFID readers.

8.5 Blocker Tag
If more than one tag answers a query sent by a reader, it detects a collision. The most important singulation protocols are ALOHA (13.56 MHz) and the tree walking protocol (915 MHz). Juels [19] used this feature to propose a passive jamming approach based on the tree walking singulation protocol, called blocker tag. A blocker tag simulates the full spectrum of possible serial numbers for tags. In [17], Juels and Brainard propose a weaker privacy protection mechanism, soft blocking. Soft blockers simply show the privacy preferences of their owners to RFID readers.

8.6 Bill of Rights
In [11], Garfinkel proposed a so-called RFID Bill of Rights that should be upheld when using RFID systems. He does not try to turn these rights into Law, but to offer it as a framework that companies voluntarily and publicly should adopt.

8.7 Classic Cryptography
1. Rewritable Memory
In 2003, Kinoshita [22] proposed an anonymous-ID scheme. The fundamental idea of his proposal is to store an anonymous ID, E(ID), of each tag, so that an adversary cannot know the real ID of the tag. E may represent a public or a symmetric key encryption algorithm, or a random value linked to the tag ID. In order to solve the tracking problem, the anonymous ID stored in the tag must be renewed by re-encryption as frequently as possible.

2. Symmetric Key Encryption
Feldhofer [10] proposed an authentication mechanism based on a simple two way challenge-response algorithm. The problem with this approach is that it requires having AES implemented in an RFID tag. In [21] we can find

a state of the art on AES implementations in RFID systems.

3. Public Key Encryption
There are solutions that use public-key encryption, based on the cryptographic principle of re-encryption. The reader interested in the precise details can read the paper of Juels [18]. Other two interesting papers that tackle the subject of re-encryption are [12] and [28].

8.8 Schemes Based on Hash Functions
One of the more widely used proposals to solve the security problems that arise from RFID technology (privacy, tracking, etc.) is the use of hash functions.

1. Hash Lock Scheme
Weis [32] proposed a simple security scheme based on one-way hash functions. Each tag has a portion of memory reserved to store a temporary metaID and operates in either a locked or an unlocked state. The reader hashes a key k for each tag, and each tag holds a metaID (metaID = hash (k)).While locked, a tag answers all queries with his metaID and offers no other functionality. To unlock a tag, the owner queries the back-end database with the metaID from the tag, looks up the appropriate key and sends the key to the tag. The tag hashes the key and compares it to the stored metaID.

2. Randomized Hash Lock Scheme
One of the problems of the previous solution is that it allows the tracking of individuals. To avoid this, the metaID should be changed repeatedly in an unpredictable way. In order to solve this problem, Weis [32] proposed an extension of the hash lock scheme. It requires that tags have a hash function and a pseudo-random number generator.

3. Hash-Chain Scheme
Ohkubo, in [27], suggested a list of five points that must be satisfied in all security designs of RFID schemes: keep complete user privacy, eliminate the need for extraneous rewrites of the tag information, minimize the tag cost, eliminate the need for high power of computing units, and provide forward security. In [27], a hash-chain scheme was proposed, in which two hash functions (G and H) are embedded in the tag. Some other recent published works on the use of hash functions are [34].

8.9 A Basic PRF Private Authentication Scheme
Molar [26] proposed a scheme for mutual authentication between tags and readers, with privacy for the tag. This protocol uses a shared secret s and a Pseudo Random Function (PRF) to protect the messages exchanged between the tag and the reader.

8.10 Tree-Based Private Authentication and Delegation Tree
One of the main drawbacks of the hash schemes already proposed is that the load of the server (for identifying tags) is proportional to the number of tags. Molnar [26] has proposed a new scheme to reduce this load, which is named Tree Based Private Authentication. This new protocol reduces the load to O(log n) but introduces the use of a Trust Center (TC). In order to reduce the burden on the TC, an o²ine delegation has been proposed [25]. Another interesting proposal is the work of Gildas and Oechslin [1][13], where a time-space trade-off is proposed.

8.11 Human Protocols
In [31], Weis introduced the concept of human computer authentication protocol due to Hopper and Blum, adaptable to low-cost RFIDs. This concept has been recently extended in an article by Weis and Juels [20], where they propose a lightweight symmetric-key authentication protocol named HB+. The security of both the HB and the HB+ protocols is based on the Learning Parity with Noise Problem, whose hardness over random instances still remains as an open question.

8.12 Non-Cryptographic Primitives
There are some solutions which do not use true cryptographic operations. The authors in [30] proposed a set of extremely-lightweight challenge-response authentication protocols. These protocols can be used for authenticating tags, but they can be broken by a powerful adversary. In [[14][16], Juels proposed a solution based on pseudonyms without using hash functions at all. The RFID tags store a short list of

random identifiers or pseudonyms (known by authorized verifiers to be equivalent). When tag is queried, it emits the next pseudonym in the list.

8.13 Low-overhead and Ultra-lightweight Solutions

The use of pseudo-randomness for increasing low-cost RFID security is often questioned because robust designs are complex to implement on low-cost RFID devices. The complexity of the implementation of robust PRNGs is equivalent to the complexity of the implementation of robust one-way hash-functions and/or equivalent encryption engines [37]. However, since the ratification of the EPCglobal standard EPC Class-1 Generation-2 (Gen2 for short) [20] and ISO standards ISO/IEC 18000-6C [28] for the usage of on-tag PRNGs on low-cost RFID devices, the number of single PRNG-based solutions has increased in the industry and academia research. The existence of PRNG hardware already deployed on most of the low-cost RFID tags justifies the convenience of this second category of security threat mitigation mechanisms.

Juels andWeis present in [36] an unidirectional authentication protocol based on the secure human identification protocol series proposed by Hopper and Blum [27]. The new protocol, called by the authors HB+, aims at preventing active attacks against the authenticity of low-cost RFID systems. The resistance of HB+ against active adversaries is proved by the authors using an statistical conjecture [13] to bound the difficulty of learning a secret (e.g., ID of the tag) given a sequence of randomly chosen vectors with embedded noisy information. The authors claim that the protocol can be implemented on low-cost tags since it only requires PRNG primitives in tags and implementation of very simple operations, such as bitwise-and and xor. Some security issues of the HB+ protocol were reported in [37]. They propose enhancements to address active attacks. However, neither the original HB+ protocol nor its sequels consider authentication of the readers and location tracking attacks. Regarding these issues, we can find in [38] a new low-overhead protocol by Karthikeyan and Nesterenko for mutual authentication of tags and readers. The requirements of this protocol are modular algebra operations, such as multiplication of matrices, and on-tag PRNG primitives. Based on similar requirements, such as on-tag PRNG and matrix algebra operations, Dolev et al. present in [17] two low-overhead proactive unidirectional protocols, called PISP (Proactive Informational Secure Protocol) and PCSP (Proactive Computationally Secure Protocol), with evolving on-tag secrets that expands indefinitely over time. Both PISP and PCSP are compared and contrasted in a joint publication appeared in [19].

The security of these protocols relies on the difficulty of recovering the operands used on both sides (tags and readers) to synchronize shared secrets. Memory space on current low-cost tags is another limitation to the security of these approaches. An enhanced version of the PCSP protocol, presented in [18], aims at preventing active attacks against the protocol while keeping similar requirements, i.e., on-tag PRNG primitives and matrix operations.

Burmester, Le, and de Medeiros proposed in [7] a new low-overhead protocol, called O-TRAP (Optimistic Trivial RFID Authentication Protocol). Like other protocols surveyed in this section, O-TRAP relies on the use of PRNG primitives in tags and some other simple bitwise operations. O-TRAP is specially designed to prevent privacy attacks while guaranteeing anonymous authentication. The protocol behaves in a manner similar to the hash-lock approach introduced in Section 2. Common secret, shared between readers and tags, are proposed in their scheme to update pseudonyms stored within tags. Like in the hash-lock approach introduced by Weis et al. in [19], readers must access back-end databases to map pseudonyms to true identities. The security of the protocol is proved using the universal composability (UC) model [8]. It is shown that the O-TRAP protocol meets the UC definition of anonymous authentication and anonymous key exchange. However, the O-TRAP protocol fails to satisfy the stronger privacy definitions, such the one stated by Juels andWeis in [37] establishing that privacy countermeasures must guarantee both anonymity and intractability. Juels andWeis point out the possibility of attacking the O-TRAP protocol by de-synchronizing tags. This allow active attacker to uniquely identify them and carry on location tracking attacks. An attack against the intractability of the O-TRAP protocol is presented

in [10]. Similar attacks exploit existing vulnerabilities in the state-of-the-art of the ultra-lightweight series of authentication protocols. Ultra-lightweight authentication protocols, such as [39], try to eliminate the necessity of hash and PRNG primitives, and involve only simple bitwise and modular arithmetic on-tag operations. The computation of costly operations, such as the generation of pseudorandom numbers, is done at the reader side. Although this fact benefits the implementation of such countermeasures on the constrained environment of low-cost RFID tags, none of these proposals seems to be resistant to either active or passive attacks. The set of authentication techniques presented by Peris-Lopez et al. in [37] were reported to be vulnerable by Li and Wang, and Li and Deng to, respectively, the de-synchronization attacks and full-disclosure attacks. Improvements of these techniques, presented by Chien in a new protocol called SASI [11] have recently been reported as vulnerable by Cao, Bertino, and Lei in [9]. These recent cases show how challenging it is to design adequate procedures given the low-cost requirement of the RFID paradigm.

9. Conclusion

In this paper two general problems have been address, the technological problems as well as the social problems involving RFID systems. Even considering that technological problems could eventually be solved, the implantation of RFID systems to a great scale will not be a reality and secured if we don't educate people about their potential benefits and risks. Taking this for granted will post a greater security risks in security.

10. References

[1] J. Waldrop, D. W. Engels, and S. E. Sanna, “Colorwave: A MAC for RFID reader networks,” in Proc. of IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, Louisiana, USA, pp. 1701-1704, 2003.

[2] Junius K. Ho. “Solving the reader collision problem with a hierarchical Q-learning algorithm,” Master’s thesis, Massachusetts Institute of Technology, Feb. 2003.

[3] Shailesh M. Birari, “Mitigating the reader Collision Problem in RFID Networks with Mobile Readers,” Kanwal Rekhi School of Information Technology, 2005.

[4] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for communication at 860MHz-960MHz Version 1.1.0, Dec. 2005

[5] S. R. Lee, C. W. Lee, “An Enhanced Colorwave Reader Anti-collision in RFID Systme,” in Proc. of The 21st International Technical Conference on Circuits/Systems, Computers and Communications 2006, Chiang Mai, Thailand, pp. 145-148, July, 2006.

[6] InChan Song, Xiao Fan, and KyungHi Chang, “Enhanced Pulse Protocol RFID Reader Anti-collision Algorithm using Slot Occupied Probability in Dense Reader Environment,” KSII Transactions on Information System, vol. 2, no. 6, pp 299-311, Dec. 2008.

[7] Cheng-Hao Quan, Jin-Chul Choi, Gil-Young Choi, and Chae-Woo Lee, “The Slotted-LBT: A RFID Reader Medium Access Scheme in Dense Reader Environments,” in Proc. of IEEE International Conferrence on RFID, Venenian, Las Vegas, USA, pp. 207-214, April 16-17,2008

[8] L. Zhang and Z. Wang, “Integration of RFID into Wireless Sensor Networks: Architecture, Opportunities and Challenging Problems,” Proc. Of Grid and Cooperative Comp. Wksps., Oct. 2006.

[9] Jaekyu Cho, Yoonbo Shim, Taekyoung Kwon, Yanghee Choi, Sngheon Pack, and Sooyeon Kim, “SARIF: A Novel Framework for Integrating Wireless Sensor and RFID Networks,” IEEE Transactions on Wireless Communications, 14:50-56,2007. [23]

[10] Joongheo Kim, Wonjun Lee, Eunkyo Kim, Kongshin Kim, and Kyoungwon Suh, “Optimized Transmission Power Control of Interrogators for Collision Arbitration in UHF RFID Systems,” IEEE Communications Letters, VOL. 11, NO. 1, Jan. 2007, pp22-24.

[11] F. Aurenhanner, “Voronio diagrams: a survey of a fundamental gemetric data strcture,” ACM Comp. Surv., VOL. 23, NO. 3, pp. 345-405, Sep. 1991.

[12] K. V.S. Rao, P. V. Nikitin, and S. F. Lam, “Antenna design for UHF RFID tags: a review an a pracical application,” IEEE Trans. Antennas Propagation, VOL. 53, NO. 12, pp. 3870-3876, Dec. 2005.

[13]. G. Avoine and P. Oechslin. A scalable and provably secure hash-based RFID protocol. In PERSEC'05, pages 110{114. IEEE Computer Society Press, 2005.

[14]. C.A. Balanis. Antenna theory: analysis and design. John Wiley and Sons, 1997.

[15]. A. Biryukov, J. Lano, and B. Preneel. Recent attacks on alleged securid and their practical implications. Computers and Security, 24(5):364{370, 2005.

[16]. CASPIAN. http://www.nocards.org/, 2005.

[17]. Auto-ID Center. 900 MHz class 0 radio frequency (RF) identi¯cation tag specifation. Draft, March 2003.

[18]. E.Y. Choi, S.M. Lee, and D.H. Lee. E±cient RFID authentication protocol for ubiquitous computing environment. In Proc. of SECUBIQ'05, LNCS, 2005. 7. T. Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In Proc. of SECURECOMM'05, 2005. 8. GS1 - EAN International. http://www.ean-int.org/, June 2005.

[19]. EPCglobal. http://www.epcglobalinc.org/, June 2005.

[20] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In Proc. of CHES'04, volume 3156 of LNCS, pages 357{370, 2004.

[21]. S. Gar¯nkel. Bill of Rights. http://www.technologyreview.com, October 2002.

[23]. P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets. In CT-RSA'04, volume 2964 of LNCS, pages 163{178. Springer-Verlag, February 2004.

[24]. O. Gunther and S. Spiekermann. RFID and the perception of control: the consumer's view. Commun. ACM, 48(9):73{76, 2005.

[25]. D. Henrici and P. MÄuller. Hash-based enhancement of location privacy for radiofrequency identi¯cation devices using varying identi¯ers. In PERSEC'04, pages 149{153. IEEE Computer Society, 2004.

[26]. ITU page on de¯nitions of ISM bands. http://www.itu.int/ITUR/terrestrial/faq/index.html, September 2005. [27]. A. Juels. Minimalist cryptography for low-cost RFID tags. In SCN'04, volume 3352 of LNCS, pages 149{164. Springer-Verlag, 2004.

[28]. A. Juels and J. Brainard. Soft blocking: Flexible blocker tags on the cheap. In WPES'04, pages 1{7. ACM, ACM Press, October 2004.

[29]. A. Juels and R. Pappu. Squealing euros: Privacy protection in RFID-enabled banknotes. In FC'03, volume 2742 of LNCS, pages 103{121. IFCA, Springer Verlag, January 2003.

[30]. A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In ACM CCS'03, pages 103{111. ACM, ACM Press, October 2003.

[31]. A. Juels and S. Weis. Authenticating pervasive devices with human protocols. In CRYPTO'05, volume 3126 of LNCS, pages 293{308. IACR, Springer-Verlag, 2005.

[32] S Pervez, I Ahmad, A Akram, S .U Swati A Comparative Analysis of Artificial Neural Network Technologies in Intrusion Detection Systems, WSEAS 2006, pages 84-89, September 22-24, 2006

[33] K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh. An ultra small individual recognition security chip. IEEE Micro, 21(6):43–49, 2001

[34] A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In 8th ACM Conf. Comput. Commun. Security, pages 103–111, 2003.

[35] S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In International Conference on Security in Pervasive Computing, LNCS, 2802, pages 454–469, Germany, March 2004. Springer

[36] An efficient authentication protocol for RFID systems resistant to active attacks. In Emerging Directions in Embedded and Ubiquitous Computing, volume 4809 of Lecture Notes in Computer Science, pages 781–794. Springer, 2007.

[37] EMAP: An efficient mutual authentication protocol for low-cost RFID tags. In OTM Federated Conferences and Workshop: IS Workshop – IS'06, volume 4277 of Lecture Notes in Computer Science, pages 352–361. Springer-Verlag, November 2006.

[38] S. Karthikeyan and M. Nesterenko. RFID security without extensive cryptography. In 3rd ACM workshop on Security of ad hoc and sensor networks, pages 63–67, USA, 2005

[39] H. Chien. SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. IEEE Transactions on Dependable and Secure Computing, 4(4):337–340, December 2007

[40] T-Y Lee, H-M Lee, H Wu, J-S Su, Data Transmission Encryption and Decryption Algorithm in Network Security, 6th WSEAS International Conference on Simulation, Modelling and Optimization, pages 417-422, September 22-24, 2006

[41] A Mahfoudhi, W Bouchelligua, M Abed

M Abid, "Towards a new approach of model-based HCI Conception" 6th WSEAS International Conference on Multimedia, Internet & Video Technologies, pages 117-125, September 22-24, 2006

[42] J. M. Correas, I.Correas and P. López, "Designing third-generation web-based systems for distance learning: influence and contributions from Open Source ",6th WSEAS International Conference on Distance Learning and Web Engineering., pages 16-19,September 22-24, 2006