International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 7, Issue 1, January - February 2018 ISSN 2278-6856

Privacy and Security Issues with RFID Technology in Ubiquitous Computing

C.Sasikala

Research Scholar, Dept.of CSE JNT University Anantapur

Abstract

Ubiquitous computing is a computing paradigm, which enables computing to be appearing everywhere using any device, in any location and any format. It includes resource-constrained mobile and wearable devices, where computations are embedded in the environment (everyday artifacts). To realize this, recently Radio Frequency Identification (RFID) technology has received a lot of attention as growing technology in the ubiquitous computing Environment. In this paper, I discuss the various sources of errors in RFID tags and some of the privacy and security issues related to RFID communication along with possible solutions.

Keywords: Ubiquitous computing, RFID , RFID tags

1. INTRODUCTION

Ubiquitous Computing (UbiCom) is a computing paradigm, where computing is made to appear everywhere using any device, in any location and any format. Here, computations are embedded in the environments [1]. Radio Frequency Identification (RFID) has recently received a lot of attention as growing technology in the ubiquitous computing Environment. Because it does not require line-of-sight alignment, it identifies the multiple tags simultaneously, and the data integrity of the original object cannot be destroyed with this tags. It has many benefits like the low cost of passive RFID tags and the fact that it works without a battery. RFID systems [4] have two main components: the RFID tag, which is attached to the object to be identified and it serves as the data carrier, and the RFID reader, which can read from and sometimes even it writes the data to the tag. The tags typically contain a microchip, it stores the data and a coupling element, which is used to provide radio frequency communication. The readers usually include a control unit, a radio frequency module, and a coupling element to interrogate the tags via radio frequency communication. Usually, in multi-tag and multi-reader environment, the tag reads may be false due to its failure of detection.

This paper is organized as follows: Section 2, describes the causes for RFID tag failures, Privacy and Security issues in RFID explained in Section 3, Section 4 , explains Security attacks and possible solutions on RFID tags and finally Section 5 provides the Conclusion of the work.

2.Failed RFID tag reads and their causes

Failure to detect RFID tags that are present in the read range of a reader can be due to a variety of reasons such as, tag detuning, collisions between the tags, air interface, tag misalignment, and metal and water in the vicinity of the RFID system. Failed tag reads caused by some of these phenomena is illustrated by Romer et al. [2] by taking playing cards with RFID tags. In addition to this some other scenarios also used to demonstrate some of the challenges involved in RFID, they believed that the playing card scenario is an ideal example because it fairly demonstrates the most common causes of failed tag reads. Figure 1 shows the RFID tags on the back of the playing cards with the RFID antenna of the I-CODE System in the background.

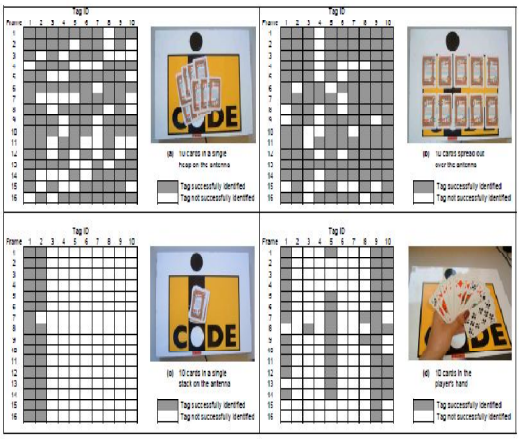

Figure1: Four different arrangements of 10 playing cards equipped with RFID tags[2]

2.1Tag Collisions

In most cases, tags that do not transfer their ID at the same time slot are not recognized. Exceptions to this rule are due to the capture effect [3], where the reader manages to properly identify the data sent with one of the tags, even though many tags react at the same time slot. In a stochastic anti-collision algorithm, there is a possibility for a tag may not be recognized for a minimum period of a single frame. Obviously, the probability of collisions increases with the number of electronic tags present and decreases with the number of available time slots.

2.2Tag Detuning

In inductively coupled RFID systems the voltage induced in the antenna coil of the tag by the magnetic field is used to power the microchip. Finkenzeller [4] explained how the tag manufacturers created a parallel resonance circuit by adding a capacitor in parallel to the antenna coil, so that the resonance frequency of the resonance circuit is tuned to the operating frequency of the RFID system. During the resonance, the resonance voltage generated throughout the

tuned tag increases as a result of increasing readability, significantly improving the outgoing bandwidth over frequencies. As a resonant application, the tag is, however, vulnerable to environmental detuning impacts which can also cause a significant reduction in reading distance. For example, a group of RFID tags that are close to each other, exhibit significant detuning effects caused by their mutual inductances. Undesirable changes in the tag's parasitic capacitance and effective inductance can also occur by metal and different dielectric mediums in the vicinity, e.g. a hand holding the tag. The change in resonance frequency away from the operating frequency results in the tag receiving less energy from the reader field and hence a decrease in reading distance. Tag detuning due to other tags that are very close it also cause the low read rates.

2.3Other Sources of Errors

Other factors of failed reads include the presence of metal in the tag vicinity environments because it distorts the magnetic flux, thus weakening the energy coupling to the tag. If the tags are attached to a metal surface, they can often not be detected at all. Similar to tag detuning, due to the antenna detuning metal in the vicinity of the reader antenna results in a read range reduction. Failed reads also caused by the misalignment of the tags with the magnetic field of the reader coil. Maximum power transfer occurs when the tag coil plane is perpendicular to the magnetic field lines. As the label is rotated concerning the field lines, the coupling is reduced until the tag is no longer identified.

3. Security and Privacy issues in RFID

To handle multiple tags reading securely and reliably, some security techniques have been developed [5], i.e. Session Concept, Enhanced Secured Protocols, Ghost Reads Improvements, Dense Readers Conditions and Covered Coding. However, there are still some privacy concerns in both user and application levels. They are also facing some security loophole in defining and managing the 'random number' key that requires attention to avoid possible privacy violations or information leakage by eavesdropping on the communication channels.

3.1 Fake Tag ID Problems

Generation 2 RFID standards uses various implementations to make sure that the incoming tag ID is in fact a valid tag ID rather than noise or glitches(ghost read). Ghost read means, a signal processor interprets noise to be a tag ID and it was a major obstacle in adopting this valuable technology. One of the drawbacks of Generation 1 RFID protocols is ghost read. As a solution to this problem Generation 2 RFID protocols come up with a 'Query' Concept. Communication between tag and reader is defined with timing constraints to create an illusion of a full duplex link. In practice, the communication is still maintained in a half-duplex mode. The tag does not speak when it reads the reader commands, but the time limits respond within a predefined time. If the tag fails to respond within the given time, the task will be terminated and the whole process must start from the beginning.

3.2Password Protection and Effective Randomness

Maintaining a secure link between reader and tag is crucial for preventing data transmitted over an air interface. In Generation 1: class 1 standards of RFID, an 8-bit password is used to execute the 'kill' command to secure the data. This 8-bit password is neither secure nor hard to break because of just 256 possible values for the password. In Generation 1 Class 0, a 24-bit password is used, which provides better protection for accessing the data. Generation 2 uses a 32-bit password, so it provides 4 billion possible values to search for the correct password. Thus, RFID achieved a level of secure communication that it never before [6].

In Generation 2, along with the password concept, a random number is used to scramble data. The tags will generate and uses a 16- bit Random Number Generator(RNG) throughout the communication session due to this we can ensure that the communication link is safe. For example, having a tag of the population up to 10,000, then the probability of generating the same sequence at the same time is less than 0.1%. In addition to 32-bit password protection, Generation 2 RFID standards use cover coding while disclosing the data with a random number to randomize the data [7].

4. Possible Attacks on RFID tags and Possible Solutions

As a technology with a convergence tendency, the RFID reader can be integrated into a hand held devices or mobile phones. These Low-cost tags led to widespread adoption of the technology and deployment on such huge scale, creates new threats to users and application privacy due to the powerful tracking capability of the tags [8]. All UHF standards provide a security mechanism for reading user memory but any reader can read the tag ID on the fly [9]. A security check should be performed on the tag before the ID is transferred and a mechanism must be defined to identify a credible reader to resolve the privacy issues.

The transmission protocol of tag reader and reader to tag communication defines the process of exchanging the data and instructions between the reader and the tag in both directions. This protocol works based on the concept of "reader talks first" and means that every tag according to UHF standards will always answer to the reader's query with its identification (ID) at first. It makes the technology powerful, and an intruder can track the reader tag. The attacker can obtain concrete product information associated with the EPC / UID code,it is available on the public network. Even though the current UHF protocols have a 'kill' command, the tag is currently dead and it will be implemented before moving it to the end users' hands, but this is not a solution for most applications. Some applications such as vehicle tracking system and personal identification systems require tags associated with objects for security purposes. Another security issue related to the tag is specified as, here the communication between a tag and a tag reader is using radio frequency, and so anyone can access the tag and obtain its output. Hence, there is a

possibility for an attacker to eavesdrop on the communication channel between tags and readers. Therefore, the authentication scheme used in RFID system must be able to protect the data passing between the tag and the reader. It means the scheme itself should provide some encryption capability [8].

Generation 2 RFID standards provide a good mechanism to transfer data securely between the tag and reader. The exchange of cover-coding was first initiated by a random number request, i.e. RN16, from the Tag. If lower secured plaintext or mechanisms are used, eavesdropping on the communication channel may break the entire security process of the cover-coding. The generation and management of this 'random number' are important for ensuring the security and integrity of the system but its size should be reconsidered and the time of command to response should be limited with precise values. So, that the random number is directly proportional to the time for the command to response. Even though, the random RN16 connection provides secure communication link, its 16-bit size still makes it susceptible, as generating 65536 combinations is very easy to find d out those combinations even with simple processors. Also, the duration of the command to response time makes it more vulnerable, it means that reader A would start querying the tag but reader B (an intruder) can join in the communication link with a fake random number.

4.1 Possible Solutions

To break the cryptosystem, any cryptanalyst must use extremely large amounts of computing recourses and time to analyze the data even if he knows the whole cryptanalytic process. One of the requirements of this cryptosystem is the property of changing few parameters that result large change of the whole system. For RFID, the cryptosystem must be easily implemented, so floating-point operations and other complicated numerical operations should be avoided.

5. Conclusion

In this paper, I discussed the concept of RFID technology along with the causes for tag failures and also the possible attacks on this communication along with some solutions. However, the major challenges for the researchers are to provide efficient, secure communication between the physical world and virtual world with less memory and power consumptions.

References

[1]. Mark Weiser, "The Computer for the 21st Century", Scientific American, Vol. 265, No. 3, pp. 66-75, 1991.
[2]. Kay Romer and Svetlana Domnitcheva. Smart playing cards: A ubiquitous computing game. Journal for Personal and Ubiquitous Computing (PUC), 6, 2002.
[3]. Jeffrey E. Wieselthier, Anthony Ephremides, and Larry A. Michaels. Exact analysis and performance evaluation of framed aloha with capture. IEEE Transactions on Communications, COM-37(2):125–137.
[4]. Klaus Finkenzeller. RFID Handbook: Radio Frequency Identification Fundamentals and Applications. JohnWiley & Sons, 2000.
[5]. Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. RFID Systems and Security and Privacy Implications. In Workshop on Cryptographic Hardware and Embedded Systems, pages 454–470. Lecture Notes in Computer Science, 2002.
[6]. Roberti M., "Understanding the EPC Gen 2 Protocol", RFID Journal Special Report, Mar. 28, 2005.
[7]. EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID, EPCglobal Inc., January 2005.
[8]. Zongwei Luo; Chan, T.; Li, J.S., "A lightweight mutual authentication protocol for RFID networks", IEEE International Conference on e-Business Engineering, Oct. 2005 PP: 620 – 625.
[9]. Garfinkel, S.L., Juels, A., Pappu, R.,"RFID privacy: an overview of problems and proposed solutions", Security& Privacy Magazine, IEEE, Volume 3, Issue 3, May-June 2005, PP:34 – 43.

AUTHOR

C. Sasikala received her B.Tech eg Degree in Computer Science and Engineering from G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India in 2009, received her M. Tech. in Computer Science from Jawaharlal Nehru Technological University University Anantapur, A.P. India in 2011. Now she is doing her research in the department of CSE in JNTUA Anantapuramu. Her research interests are in the fields of Cloud Computing andnetwork security.