CHAPTER (1)

Introduction

Chapter 1

This chapter introduces a wide background about the Radio Frequency Identification (RFID), and presents the major building block and the architecture of RFID system, and finally the chapter presents the main contributions of the research work and the thesis outline.

1.1 Research Motivation

RFID is the future of identification technology, it uses radio waves to identify objects by attaching RFID tag to the object that needs to be identified, and this process is done by transferring data between the RFID reader and RFID tag.

RFID system building block consists of six basic components (Reader, Tag, and Database, Servers, Enterprise Application and middleware).

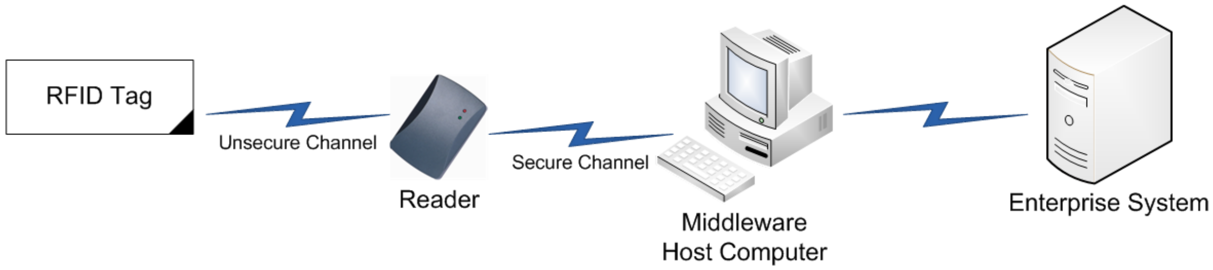

Figure 1.1: The Block Diagram of RFID system.

RFID system components have various types and standards; there are two types of readers: fixed RFID reader and mobile RFID reader, and everyone has its own function and applications. The RFID tags have three types passive, semi-passive active. The main difference between them is that the passive doesn't have any power source; it gets the power from the radio waves sent by the reader, while the semi passive and the active tags have their own power sources which are an onboard battery that broadcasts the signal.

RFID systems have many advantages over the existing identification system that used nowadays like barcode systems and biometric ones. The main difference between the barcode and the RFID system is that the barcode system identifies the type of the item only, but does not distinguish between two items with the same type. while the RFID system tag has its unique identification number and therefore, can distinguish between multiple items of the same type. Some of the RFID tags can be simultaneously read few meters far and also several tags unlike the barcode needs centimeters far and only read one at a time . There are also disadvantages of RFID system which have some security risks like lack of confidentiality, privacy, integrity and the easiness of illegal tracking.

All these issues must be carefully considered in any new proposed system. In addition, the cost of the system and its efficiency must be taken into account in the implementation of such systems, to help overcome the security risk issues.

There are many proposed protocols aimed at overcoming the security risks, which are applied to the RFID system. Those proposed protocols are classifying according to the operations that can be done on the tag, depending on the level of security needed in the system. There are some limitations to implementation of the RFID system; they are: storage space capacity available, performance, power consumption need.

RFID systems are currently used in different applications that aim to automate the processes and to reduce the human interference. They are widely used in supply chain management to improve the performance and efficiency of the inventory tracking and management systems, also in the healthcare fields where the RFID are used to improve the patient’s safety and reduce the chances of leaving surgical tools unintentionally in surgeries. In the last few years, RFID was used to tie the physical world to the virtual world. RFID in Social Media first came to light in 2010 with Facebook's annual conference; all attendees of the conference have received special RFID tags that enable them to check-in to various locations throughout the conference places, the service lets attendee tag himself in photos, become a fan of various Facebook Pages, and share activity to his/her Facebook profile, but it’s still a concept service.

1.2 Thesis Definition

Many RFID protocols have been proposed recently and each of these protocols can be classified according to the RFID tag resource required by the protocol, Hung-Yu Chien who is head of department of information management, national Chi Nan university classifies the authentication protocol into four classes depending on the resources required.

1- “Full-fledged class”.
2- “Simple class”.
3- “Lightweight class”.
4- “Ultra-lightweight class”.

Hung-Yu Chien proposed an ultra-lightweight authentication protocol SASI (Strong Authentication and Strong Integrity) which aims to secure the communication channel between the tag and the reader, SASI protocol consists of three phases:

1- Tag identification phase.
2- Mutual authentication phase.

3- Pseudonym updating and key updating phase.

Each tag keeps (ID) unique static identification for each tag in nonvolatile memory and must save in rewritable memory two entries:

1- (IDS) pre-shared a pseudonym.

2- (k1, K2) two keys.

The two entries are used in communication between the reader and the tag. When the first entry the potential next value, is not found in the backend database, the reader requests the old value from the tag. And if it is found, the reader fetches the corresponding variable to communicate with.

Hung-Min Sun, Wei-Chih Ting, and King-Hang Wang have found out that there are two de-synchronization defects that can be utilized to break SASI protocol.

1- The first attack will de-synchronize the tag in three steps:

a. First step: let the reader and the tag communicate and record message between them and interrupt the communication, so the tag will updated and the reader will not.
b. Second step: let the reader and tag to communicate again without any interruption.
c. Third step: after the reader leaves the reading range, the attacker initiates the connection with the tag and attacks it, and now the reader and the tag in out of synchronization.

2- The second attack will de-synchronize the tag in two steps:

a. First step: let the reader and the tag communicate with each other without any interruption and the attacker will eavesdrop on the message exchanged between them.
b. Second step: is to forge a tuple in the message recorded and send it to the tag many time and the tag accepts it and responds to the attacker and now the tag and the valid reader is out of synchronization.(maximum number if tries is ,96 limited)

1.3 Main Contribution

1- This thesis first explains in details the SASI protocol and the communication process between the reader and the tag. It also illustrates how authenticate each other and the messages exchanged between them. It introduces the attacks that de-synchronize SASI protocol and the two modifications proposed scenarios to prevent de-synchronization attacks that break through the SASI protocol.

2- the implementation takes place in two phases:

a. The first phase: in this phase we implemented SASI protocol on which our work is built, which was not implemented by Chien. After that, the implementation for the two attack scenarios to verify they can break SASI protocol.
b. The test was conducted as follows :
c. One tag was attacked 10 times; number of tags put to test was increased by tens till we conducted the test on 100 tags at the same time. All these tags were 10 times attacked results were recorded as shown in the following chapters.

The second phase: the proposed modification was implemented the two attack scenarios were applied to break through the SASI protocol; results were recorded same as we did in the first phase.

3- By comparing the required storage capacity for SASI with the proposed modification on SASI protocol we found that SASI required storage capacity =576 bits. in our modification is the same, so it can calculate the total number of bits required by defining the number of tuple needed to be stored, so it will require storage space by (96 x (3 x n)) = bits where n is the number of tuples needed in each modification scenario and 96 bits for the length of each variable, and (3) is the number of variable in each tuple that stored in the tag memory.

4- Finally, the comparison of the communication cost between SASI protocol and the proposed modification scenario is summarized in the following points:

   a. SASI protocol performs tag identification phase and mutual authentication phase in four messages:

      i. 2 messages sent in the tag identification phase.

      ii. 2 messages sent in mutual authentication phase.

   b. The Proposed Modification performs the tag identification phase and mutual authentication phase in four messages:

      i. 2 messages sent in the tag identification phase.

      ii. 2 messages sent in mutual authentication phase.

   We have proposed seven modifications that have a little change in the tag identification phase; their behavior is different from that of the SASI protocol.

5- After the implementation we compared the results of the proposed modification with SASI, and we found that the performance analysis for our modification is almost the same as the SASI protocol.

   a. The original SASI protocol does not resist but the modified one with the different scenario resist the de-synchronization attacks.
   b. The original SASI protocols does not resist but the modified one with the different scenario resist the of disclosure attacks.
   c. Privacy, anonymity, mutual authentication and forward secrecy were achieved by SASI protocol and all modified scenario
   d. Total number of messages for mutual authentication in SASI (4L) in proposed modification scenario ranged from (4-5 L) L size 96 bits.
   e. Memory size on tag for SASI is (7L)), in proposed modification scenario (1+ (3 x n)) L.
   f. Memory size for each tag on server backend database for SASI is (4L) in proposed modification scenario (1+ (3 x n)) L.

1.4 Thesis Outline

This thesis is structured as follows:

Chapter 2 presents RFID systems with its frequency range used, and the existing standard used in communication, it also introduces privacy and security in RFID system and presents a survey for RFID protocols.

Chapter 3 explains the one of the ultra-lightweight authentication protocols and its proposed attacks and also the two scenarios proposed of modification to prevent vulnerabilities or attacks on SASI (Strong Authentication and Strong Integrity).

Chapter 4 describes the development of the proposed functions that are different scenario aimed at preventing the attacks on SASI, and compute the communication cost and storage required for each scenario. It also reflects the performance comparison between the ultra-lightweight authentication protocols and the proposed scenarios.

Chapter 5: summarizes the conclusion of the work and proposes some recommendations for the continuity of the research and future work in this field.

Appendix A: presents the class diagrams for the source code that describes the relation between each object and the type of each object in the whole system. Also it describes the classes' attributes, and their functions relationship with other classes.

The following chapter, chapter (2), introduces the RFID systems in brief of each component which the system consists of, the frequency range used by RFID system and a listing of the existing RFID protocols with privacy and security.