RFID: Promises and Problems

Arjun Agarwal and Mala Mitra
PES Institute of Technology, 100 Feet Ring Road, BSK III Stage, Bangalore, India 560085.
Emails: arjunagarwal1985@hotmail.com, mala.mitra@pes.edu

Abstract: With the advent of wireless technology, a rapidly advancing area is that of Radio Frequency Identification Devices or RFID. RFID technology was first developed as an espionage device during World War II. However, nearly 30 years of research was required before it became a part of our everyday lives.

Informally, RFID can be considered a non-contact method of using radio frequency electromagnetic waves (with frequencies up to 2.5GHz) for communication between 2 remote entities. Data is stored in devices called RFID tags or transponders, and is retrieved by readers. Each tag stores a unique identification number. The main purpose of RFID is automated identification of people and products.

The advantages of RFID over conventional identification systems are many. RFID also allows us to think of applications hitherto undreamed of. The biggest stumbling blocks in the use of RFID are the numerous and complex security threats that are involved with RFID, as well as privacy issues that have human rights organizations up in arms. Also, there are few standards that have been agreed on, and many protocols are still in nascent stages of development. This limits the practical usage of RFID today. In addition to the potential scope of RFID applications, the security threats that still have to be satisfactorily countered make RFID Security a field that is being widely researched.

This paper starts with a hypothetical situation that we may be faced with in the future. It then goes on to give details about RFID systems. Some applications of RFID are enumerated, as well as the advantages RFID has over conventional systems. Finally, some of the security threats facing RFID are explained.

Index Terms: Applications of RFID, RFID Security and Privacy.

I. INTRODUCTION

Customer care in 2020 when the use of RFID devices is widespread

Waiter: "Thank you for coming to Pizza Hut."
Customer: "Can I order my meal?"
Waiter: "Sir, I've already scanned your RFID tag using my portable reader. Please wait. OK, you're Mr. John, and you're from 17 Birch Road. Your home number is 40941 2366, your office number is 76452302 and your mobile number is 0142662566.
Customer: "How did you get all my phone numbers?"
Waiter: "We are connected to the system sir."
Customer: "What do you have on your seafood pizza?"

Waiter: "A seafood pizza may not be the best idea sir."
Customer: "Why is that?"
Waiter: "According to your medical records, you have high blood pressure and even higher cholesterol levels."
Customer: "What? What do you recommend then?"
Waiter: "Try our Low Fat Hokkien Mee Pizza. You'll like it."
Customer: "How do you know for sure?"
Waiter: "You borrowed a book entitled "Popular Hokkien Dishes" from the National Library last week sir."
Customer: "OK I give up. Bring us three family size ones then, how much will that cost?"
Waiter: "The total is $49.9"
Customer: "Can I pay by credit card?"
Waiter: "I'm afraid you have to pay us cash sir. Your credit is over the limit and you have owed your bank $3,720.55 since October last year. That's not including the late payment charges on your housing loan."
Customer: “Are you sure you’re supposed to know all this?”
Waiter: "It’s freely available on the system sir. Anyone can access it. Will there be anything else?"
Customer: "Nothing. By the way, aren't you giving me the 3 free bottles of cola as advertised?"
Waiter: "We normally would, but based on your records you're also diabetic..... "

Imagine this happens to you in the future. The advantages are apparent. For example, you walk into a restaurant and you don’t even need to order – they know what you like! They won’t serve anything you’re allergic to either. When you walk into a hospital, there is no need for you to bring your medical file, as the doctor will immediately know your history. These are just a few examples of the scope of RFID.

The problems though are as glaring. Not many would like their personal information being available at everyone’s fingertips, as the scope for misuse is vast. For example, personal information maybe used for blackmail. Thus, there are many issues that still have to be addressed before RFID is widely used.

II. RFID SYSTEMS

An RFID system basically consists of three components:

1) The RFID tag or transponder (derived from transmitter/responder). It bears the information that identifies the person or object, and is carried or implanted. The information is usually in the form of an alphanumeric word. This information is called an identifier, and that of each tag is unique. Tags vary in size, and their size mainly depends on the size of the antenna on the tag.

2) The RFID reader or transceiver (derived from transmitter/receiver). It supplies energy to the tag in the form of RF electromagnetic waves. It then receives the signal from the tag. It usually contains an interface that allows it to communicate with a data processing system.

3) The back-end infrastructure or data processing system. This receives the information from the reader, and processes it. An example is a system with a product database that uses the tag ID number of a product to identify the product.

The RFID reader and the back-end infrastructure are together called the reader system. A schematic of an RFID system is shown in Fig. 1.

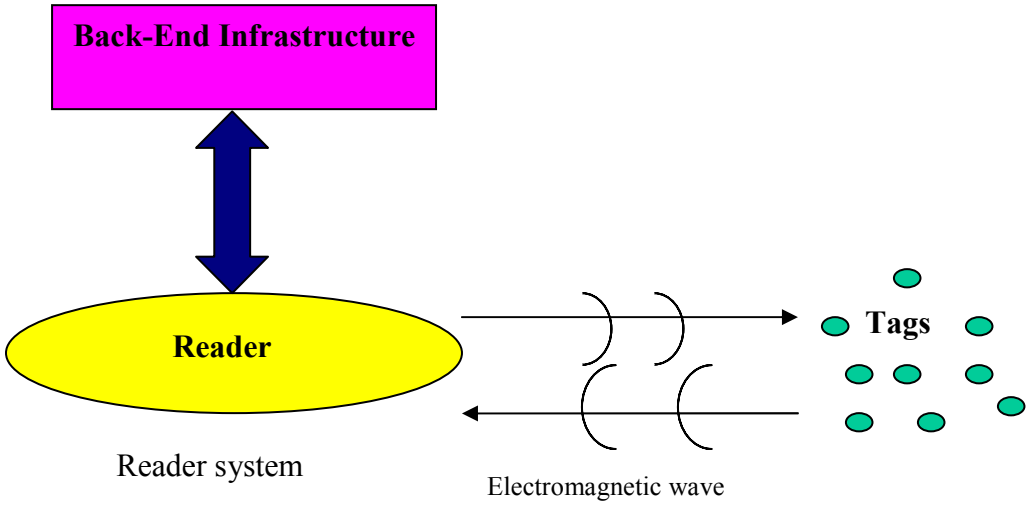

Fig. 1: Typical RFID System Components

Whenever a tag comes into the vicinity of a reader, it receives a signal from the reader and transmits its unique key, enabling identification of the object or person carrying the tag. Clearly then the reader must be able to handle multiple tags at once. There are some cases, however where there is only one tag for a particular reader. Thus RFID systems are of two types – one to one and many to one.

A. Tag Types:

RFID tags can be classified into 3 types depending on their power consumption: passive, semi-passive and active.

Passive tags have no internal energy source. The electrical energy required for the tag current is derived from the radio waves emitted by the reader. These tags are the smallest and cheapest, and thus are the most widely used. They also have a virtually unlimited lifespan.

Semi-passive tags are similar to passive tags in that the energy required for transmitting the signal is still derived from the reader. However, these tags have a small battery for internal computations.

Active tags do not require external power. They have an internal battery that is used for transmission of data as well as for transmission of the signal. As a result of the

increased power, they can transmit data over a much larger range compared to passive tags. However, their relatively high cost means widespread use is not possible.

The tags which will most likely see the largest growth in the near future, especially in applications where tags are to replace bar codes, are passive tags.

B. Frequency of Operation:

RFID systems operate in several frequency bands. The low frequency (LF) band is 124-135 kHz. HF ranges from 3 MHz to 30 MHz, with 13.56 MHz being the typical frequency used for HF. UHF ranges from 300 MHz to 1 GHz. Microwave frequency ranges upward from 1 GHz. A typical microwave RFID system operates either at 2.45 GHz or 5.8 GHz, although the former is more common. A detailed discussion on used frequencies and their relative merits and demerits is given elsewhere in the techonline journal [1].

C. Read Range:

By read range, we mean the maximum radius around a reader in which, if a tag is brought, its identifier can be read successfully by the reader system. Range depends on many factors:

- Frequency of operation: Range increases with frequency. However, metal acts as a barrier to radio wave propagation, and reduces the range at higher frequencies.
- Transmitter power of the reader.
- Antenna size of reader and tags.
- Transmitter power of tags: This is applicable only for active tags.

Often, vendors of RFID readers are required to quote a range. They either quote it for standard tags e.g. tags manufactured according to ISO standard, or specify the tag particulars.

III. RFID APPLICATIONS

The main purpose of RFID is automated identification of products and people. One of the biggest advantages of RFID over conventional systems such as bar codes, is that neither line of sight nor physical contact is required for an object with an RFID tag to be identified, as is the case with bar codes where line of sight is required and smart cards, where contact is required.

It is hoped that RFID tags will become widely used, replacing all manner of current identification as well as introducing applications not dreamed of earlier. One of the reasons is that the prices of RFID tags have been falling steadily. RFID tags are viewed as the next generation successors to bar codes. This makes it necessary for their cost to be low, as they will add to the cost of the item on which they are included. To the best of our knowledge, the cheapest tags available in the market cost $.07 cents per tag, if they are bought in volumes of 10 million [2] as of February 2006. The cost seems likely to drop to $.05 in the near future [3]. From a financial point of view, such prices would facilitate the use of RFID in all manners of applications where identification is required.

As mentioned, the main application of RFID is for automated identification, and it is hoped that RFID devices will replace all manners of optical identification techniques. To explain the numerous advantages RFID possesses, we include here in Table I a comparison of RFID tags and barcodes [4] for quick reference.

Table I: A comparison between Bar Codes and RFID tags:

Bar Codes	RFID Tags
1. Bar codes require line of sight to be read	RFID tags do not require line of sight to be read.
2. Bar codes can only be read one at a time	RFID tags can be read virtually simultaneously
3. Physical condition important, e.g. cannot be used in dirty environments	Physical condition not important
4. Bar codes can only identify the type of item	RFID tags can identify specific items.
5. Bar code information is static	RFID information can be updated

With reference to Table I, the advantages of RFID tags over bar codes are explained below.

1. In order for a barcode to be read, the infrared wave from a reader must fall on the barcode. Hence, barcodes can only be read if they are in a specific region, or line of sight of the reader. This is not required for RFID, as the radio waves emitted by the reader can activate the tag anywhere in the reading range.
2. As each barcode has to be in the line of sight of the reader, only one bar code can be read at a time, reducing the speed at which the bar code information is processed. By contrast, even if there are up to a hundred [4] tags in the read range of the reader, each can be read, and the speed at which they are read will make it appear to us that the reading is simultaneous. This would require the use of the many to one topology mentioned earlier, as well as the implementation of an appropriate protocol. This is feature is especially advantageous in access control using RFID.
3. If barcodes are scratched or dirty, they cannot be read as the reader cannot identify the reflected optical signal. The physical condition of RFID tags is not important, because the information is transmitted using radio waves, which will propagate even if the tag is dirty.
4. Each type of item has the same barcode. For example, every copy of Dan Brown's book The Da Vinci Code has an identical barcode. If, however, books are tagged with RFID devices, then each book will have a unique identification number, and if two of us buy the book, the identification number for each book will be unique. This will, for example, enable tracking of defective items in supply chains.
5. Barcode information cannot be updated, as the barcode is printed on the item. In the case of RFID tags, the data is electronically stored and hence can be updated.

A. Typical Applications of RFID

A.1 Supply chains and retail services: One of the widest uses of RFID today is in supply chains. USA's retail giant, Wal-Mart, has ordered more than a million of its products to be tagged with RFID devices [5]. A related application is the tagging of consumer products in retail outlets – widespread implementation however will have to wait for a few years, as a result of a number of privacy issues [6]. As we have seen, each RFID tags uniquely identifies an object, rather than a class of objects, and this prevents many illegal activities during supply. Consider, for example, a retail outlet ordering 10 boxes of medicine with RFID tags from 5 different suppliers and selling them to consumers. The next day, a consumer returns to the shop complaining that the box was only half full. By reading the RFID tag on the box, the retail outlet is able to determine exactly which supplier the defective box belongs to, which would not be possible if the box had had a barcode printed on it. Use of RFID tags for consumer goods would enable check out lines to move faster as simultaneous reading of tags is possible.

A.2 Access Control: Many access control devices currently used are based on smart cards, which have to be swiped in a reader. The use of RFID for access control would mean that removal of the card from a pocket is unnecessary, making it more convenient for the user. Use of RFID also makes control systematic. By systematic we mean that two people accessing an area at the same time should be recorded. For example, if access control uses smart cards, then if one person opens a door using a smart card another authorized person can slip in behind him, without the system having a record of it. If however, RFID tags are used, then as soon as a person with a tag comes into the read range, the reader detects the person. An example of such a system was implemented by Texas Instruments (TI) in 1999 [5]. They developed a wireless access system for ski lifts. As soon as members with a valid RFID tag came near the lift, the ski car opens and they can climb on. An automatic log of the people using the lift is also maintained.

Another access control area where RFID has found popular use is that of car keys. Companies such as Mercedes Benz are implanting tags in keys, and a reader in the car. When the person with the key comes near the car, the door automatically opens, without having to insert the key. Some cars even have multiple keys. This is useful if there is more than one person who drives the car. Each person saves his preferences with reference to seat position, cabin temperature etc. Depending on which RFID tag is read, the onboard system changes the various parameters in the car to suit the person whose key it is.

One last example, which has been implemented successfully in many cities around the world, is the use of RFID in toll gates. Frequent commuters place an RFID tag on their dashboard. When they approach the gate through a special lane, a high-ranged reader reads tag and allows them through. Each time the tag is read, the amount of "currency" left in the user's account is decreased, and when the currency gets over, the user buys a new tag.

A.3 Sub-dermal Tags: This refers to tags that are implanted under the skin of people or animals. TI has implemented several systems for animal tracking. RFID tags are especially useful in tracking cattle, as well as keeping a count of a herd. Tags can also be used to study migration patterns of fish, by tagging them and keeping track at regular intervals using a powerful reader on a ship.

Recently, the number of people who have been getting RFID tags implanted has also been on the rise.

There are a number of forums on the Internet where people who have been tagged discuss their experience [7]. One typical example is for computer access. Instead of typing in a user name and password, a user has a tag implanted under his palm, and simply has to wave his hand in front of the monitor, which has an RFID reader inbuilt.

A.4 Tags in Libraries: Some libraries have implanted RFID tags in their books. This allows users to carry out returning and borrowing applications themselves. Librarians can also detect missing and misfiled books easily, by using a hand held battery operated RFID reader. Then, the books on each shelf do not have to be removed to check which belong there and which don't, only those shelves that cause the RFID system to show an error can be checked. According to Bibliotheca Library systems [8], more than 100 million books world wide in libraries across Europe and North America have already been tagged.

A 5 Smart Appliances:- A potential use of RFID devices is in smart appliances. Though these have not yet been developed, there is a lot of speculation on them, and smart appliances are probably one of the most exciting areas of RFID. Here we cite a few examples.

-Clothes made of a particular material can be implanted with tags with ID numbers in a particular range. When these clothes are placed in a washing machine with an RFID reader, the machine automatically selects the number of cycles, amount of water etc.

-Consider the following scenario – you buy a packet of microwave popcorn implanted with an RFID tag. You go home and place it in your RFID enabled microwave, and as soon as you do so the microwave automatically sets the time required and starts operating!

-Your refrigerator contains an RFID system, and all food products are tagged. The RFID system can communicate with a central database that holds the information for the food products. The reader reads the information and is able to determine information such as the expiry date for a particular carton of juice. When the date is reached, an alert is sounded, saving you from having the expired juice!

IV RFID SECURITY AND PRIVACY ISSUES

Consumer concerns regarding RFID can broadly be classified into security and privacy. Security issues deal with legitimate readers getting information from illegitimate tags, whereas privacy issues deal with illegitimate readers getting information from legitimate tags. From a consumer's point of view, the privacy issue is more important, and as a result media coverage has been much higher. However, recognition of the importance of RFID security has also been increasing.

The issue of RFID security can often seem paradoxical in nature. While the use of RFID increases security in some areas, the very nature of RFID communication poses a number of new privacy and security risks.

Use of RFID certainly has the potential to augment security in certain areas. Implanting RFID tags in money will act as a deterrent to counterfeiting and fraud. We have already seen in Section A.1 how the use of RFID helps retailers track down dishonest suppliers. RFID tags are already used in clothes in departmental stores to prevent theft. When an item is sold, the RFID tag is removed. All customers have to walk

in the read range of a reader before leaving the store. An alert sounds if a person walks out of the shop with clothes from which the tag hasn't been removed, thus nabbing would-be thieves. Implanting RFID tags in animals can help recover pets that have been stolen.

Despite all these benefits, opposition to the use of RFID is increasing. More and more consumer groups are protesting, saying that consumer privacy will be threatened. RFID security has even come up for discussion in several US states. One of the most vocal consumer groups against the implementation of RFID in retail stores is "Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)" headed by Katherine Albrecht (referred as KA from here). Albrecht states two examples, one of which is hypothetical, where consumer privacy is abused [9].

- **KA:** "Let's say I buy a pair of size 7 women's Nike running shoes with a credit card. Currently, most major national chains are recording information about what people are buying. In the future, however, my pair of size 7 Nike running shoes will have a unique ID number in an RFID tag embedded in the sole—unless we stop it—so anytime that I step on carpeting or a floor tile that's been equipped with an RFID reader, it can scan that number and know: "Hey, I'm at the Atlanta courthouse, and I just saw shoe number 308247 step by. Let me cross-reference that in the database. That's the shoe that was purchased by Katherine Albrecht."
  And shoes are a particularly interesting example to think of in that regard because we don't trade shoes with other people, for a variety of hygiene and fitness reasons, and most of us tend to wear only a few pairs of shoes regularly. So if you can identify a pair of shoes as belonging to an individual and strategically locate reader devices—put them in the entrance to the airport, the entrance to the courthouse, the entrance to the Wal-Mart store—you can pinpoint the time and place at which a person was seen entering that location. That opens up a whole new horizon of tracking capability to watch people, for marketers and homeland security folks.
- **KA:** "The Metro, the RFID industry's showcase retail outlet in Germany, is a good example of a retailer abusing RFID in a surreptitious way. About a year and a half ago, we toured the store for over three hours. The next day I was giving a talk to a group of Germans on privacy and RFID. We had set up a $200 reader device we had bought off the Internet to read the RFID tags off the Pantene shampoo and the Gillette razor products and just on a lark, one of my colleagues held his frequent shopper card up to the reader device and a number appeared on the screen. We found out that they had actually tagged us—and apparently 10,000 other shoppers—at the store, by giving out these cards without being told that they contained RFID tracking devices. Retailers will be able to identify you from the moment you walked in the door. They could identify your value to the store and then treat you differently depending on how profitable you are."

We now turn to specific examples of threats to privacy and security as a result of usage of RFID tags.

A. Issues relating to privacy

A.1 Tracking: Tracking refers to clandestinely following a person's movements without his or her explicit permission. RIFD tags usually emit a constant identification number or an alphanumeric called as a key. If an individual has a tag somewhere on his person, he

can be tracked by anyone holding a portable reader. As mentioned earlier, the read range can be increased by using a higher power reader, and using the key emitted by the tag, the victim can be followed at a distance. Fixed readers can also be used as in the case of the Nike shoes proposed above to know where a person has been. Supporters of RFID note that other technologies such as Bluetooth also allow tracking. However, we observe that devices such as mobile phones can be turned off. This option is not available in the case of RFID, as the tags can always be read if a reader is present. Clearly, encryption too does not solve the problem of tracking. Even if the tag ID number is encrypted, the encrypted key emitted by the tag will still be constant, and will allow the tag to be tracked.

In order to overcome the problems posed by tracking, several solutions have been proposed.

- Killing of tags, wherein the tag is permanently deactivated when the consumer leaves a store is one proposed method [6]. Then, tracking will be avoided. However, all the post-buying benefits, such as those described above with respect to smart applications, will be lost. Another method proposed is sleeping of tags, wherein the consumer can reactivate a tag using a PIN. Clearly though a very large number of PINs are required, one for each tag, and so management will become difficult.
- Another approach proposed by Ari Juels is that of minimalist cryptography [10]. When implementing cryptography for RFID systems, the limited memory and processing capability of tags must be kept in mind. Juels proposes that each tag have a number (say ‘n’) of different identifiers i.e. a set of identifiers unique to itself. Each of these identifiers is called a pseudonym. Each time the tag is interrogated, it sends the next identifier in the set, and once all the identifiers have been exhausted, the first repeats. In order to prevent adversaries from getting the entire set of identifiers, it is proposed that data emissions are “throttled” – there is a time lapse between each response of the tag so that quick fire interrogation is not possible.

  To further enhance this scheme, a modification proposed is that after all the pseudonyms are exhausted after ‘n’ queries, the set of pseudonyms is refreshed by the reader, so that a new set of pseudonyms is stored. Suppose an adversary queries the tag ‘n’ times. After the tag list is refreshed, if the same adversary queries the tag, it will now appear to be a different tag, as its pseudonyms are different. However, one difficulty is ensuring that all legitimate readers are kept up to date with regard to when each tag is refreshed, and which set of pseudonyms identifies which tag.
- A scheme called blocking has also been discussed by Juels in [11]. Special tags called blocker tags have an additional bit called a privacy bit. If the bit is ‘0’ the tag can be scanned and if the bit is ‘1’ the tag cannot. It makes use of the anti-collision protocol that is used to allow simultaneous reading of tags. In a protocol called the tree walking protocol, tags are represented by a binary tree. If the first bit of a tag identifier is ‘1’ it lies in the right half of the tree, and if the first bit is ‘0’, it lies in the left half. Then, the next bit is checked and so on. If the privacy bit is set to ‘1’, then the tag emits both, a 0 and a 1. This forces the reader to scan

both halves of the tree, and if the tag identifier is 96 bits long, the reader has to scan billions of tags – effectively preventing identification of the tag.

- Another scheme discussed by Avione [6] is that of re-encryption. He proposes that each time the tag is read, the reader use a different method of encryption to encrypt the identifier. Say there are 4 different encryption schemes, then each time the tag is read the next scheme in the list is used to encrypt the identifier. A drawback is that it is difficult for the reader to determine which scheme has been used for encryption when it reads the tag. Also, if an illegitimate reader reads a tag a number of times, it will be able to determine that though the identifiers appear different, they in fact represent the same tag.

A.2 Information Leakage: Information leakage refers to when the tag reveals information that is potentially sensitive, and can be used to determine the exact nature of the object. For example, a consumer in a fervently capitalist company may buy the book 'Das Kapital', Marx's famous treatise on communism. If this book is implanted with an RFID tag, any government agent with a reader will be able to read the tag identifier, and by accessing a central database will know the name of the book. This consumer may then be persecuted, as he may be suspected of being a communist. Similarly, a person may buy medicines implanted with RFID tags. Again, by reading these tags it is possible to know the exact nature of a person's ailments, which is sensitive information. In a famous case, RFID tags were used in toll gates as described above. A court ordered the access information to be opened to determine the movements of the defendant in a divorce case, which finally led to the defendant losing the case.

Many legal methods have been proposed to overcome this problem. For example, to restrict illegitimate readers, it has been proposed that reader ranges be restricted. However in our view this will not deter a criminal, as they will just illegally increase the range of the reader. Another bill was introduced in California. It recommended several modifications to RFID tags, such as requiring that RFID tags be optically scanned before they emit their identifier. However, this nullifies the very benefit of RFID – we may as well stick to optical methods of identification!

In the case of information leakage, it is of course possible to talk to encryption as a solution. If the identifier is encrypted, a rogue reader will not be able to use it to identify the article. One of the biggest advantages of the re-encryption scheme discussed above in section A.1, that it addresses both, the problem of tracking and information leakage to an extent.

B. Issues relating to security

The issues relating to security are often those that involve fake or illegitimate tags, rather than readers. The main security problem is that tags can very easily be counterfeited or copied. This allows impersonation of tags and gives rise to a host of problems. Imagine we are in an age that people are implanted with tags, and these tags are used for everything form access control to ATMs to credit card payments. If an adversary copies the tag of another person, then it would be easy for him to access the victim's bank accounts and withdraw money.

Consider another example, of a dishonest company called Company Z. Suppose it handles shipment of goods from point A to point B, and each crate of goods is implanted with an RFID tag. Company Z would find it easy to make a copy of a tag on a crate, and replace that crate with an empty one implanted with the counterfeit tag. They could then

steal the original crate with the goods in it, and the fact that the crate arrived empty will be blamed on the suppliers!

One particular kind of attack is referred to as Relay Attacks, which threaten access control systems. This involves the use of an illegitimate tag B as well as a rogue reader. Suppose the original tag A and reader (which is at the restricted area) are some distance apart. The fake reader reads the original tag, and uses this information to program B with A's identifier. B then acts as A and communicates with the legitimate reader to obtain illegal access to the restricted area. A schematic is shown in Fig. 2.

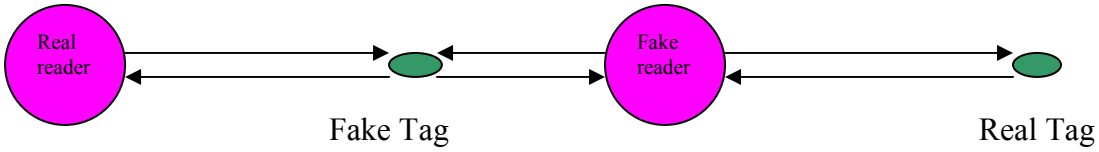

Fig. 2 Relay Attacks

As we have already stated, most of the current research and literature deals with privacy issues rather than security ones. However, security issues have been addressed by Juels in [11]. He states that anti-counterfeiting measures are difficult in tags that are general purpose. Methods are discussed whereby it would be possible for a tag to hide information that cannot be accessed until it is activated by the user of the tag. Thus, a simple copy of the tag would not possess all the information to allow successful communication with the reader.

V. CONCLUSION

The development of RFID has opened whole new vistas for the future, making it possible to imagine a consumer life of enviable ease. However, before these dreams become a reality, the privacy and security problems thrown up by RFID need to be addressed.

In this paper, we have been able to discuss a few aspects of RFID security and privacy, as well as the enormous scope RFID offers. It is hoped that we have been able to give a flavor of the work that is currently being done, and that we have also shown how much work is still required.

REFERENCES

1. Sandip Lahiri, RFID: Technology Overview, Available at http://www/techonline.com
2. Wikepedia, the free encyclopedia. Available at http://en.wikipedia.org/wiki/RFID
3. S Sarma. Towards the Five Cent Tag. Auto-ID Center White Paper MIT-AUTOID-WH-006, 2001.
4. RFID Road map. Available at: www.rfidroadmap.com
5. Texas Instruments. Available at: www.ti.com
6. Gildas Avoine. Cryptography in Radio Frequency Identification and Fair Exchange Protocols – PhD thesis. Available at http://lasecwww.epfl.ch/~gavoine/
7. http://tagged.kaos.gen.nz/
8. Bibliotheca RFID Library Systems. Available at: www.bibliotheca-rfid.com

9. Total Surveillance. Available at: www.motherjones.com
10. Ari Juels. Minimalist Cryptography for Low-Cost RFID Tags . Available at: www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs
11. Ari Juels. RFID Security and Privacy – A Research Survey. Available at: www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs
12. S Sarma, S Weis and D 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.
13. Martin Feldhofer. "A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags", in IEEE Proceedings of MELECON 2004, Vol. 2, pp. 759–762, ISBN 0-7803-8271-4, Dubronvnik, Croatia, May 12-15, 2004.
Available
14. RFID Journal – White Papers. www.rfidjournal.com
15. http://tagged.kaos.gen.nz/7
16. The RFID Weblog. http://rfid.weblogsinc.com/