RFID privacy protect using blocker tag with anti-blocker tag scheme

Wen Chen, Wen-Nung Tsai

Contents

List of Figures

中文摘要

無線射頻辨識系統（RFID）廣泛的應用在現代的生活中。 然而RFID系統卻有隱私和安全性的問題等待解決， 學術上有非常多隱私和安全性相關的研究， 尤其是在無線網路上面的相關研究非常豐富， 但是這些不一定都適用在RFID系統上面。 因爲大部分的方法都需要較多運算資源的硬體來支援， 或是一旦使用了這些方法，就會失去人們使用RFID的方便性。

Blocker tag是對於隱私權保護的一個解決方案。 他是一種基於網路防碰撞的演算法。 利用這個演算法的弱點來保護tag不會被讀取。 他可以非常有效的防止個人資料遭到竊取。 但是一旦這個方案被人惡意的濫用， 人們就可以巧妙的避過結帳掃描等，可能會造成商業或作業損失的缺失。 對於RFID面對的全球性應用來講， 將會是一個很嚴重的問題。 而如何去偵測出是否有人惡意的使用這樣的方案， 即本篇文章主要探討的問題。

Keywords: anti-collision, blocker tag, RFID, privacy, inventory

Abstract

Radio Frequency Identification (RFID) technology is widely used in modern application. However, the RFID system has some privacy and security problems.[17] Although there are many researches on wireless network related to the privacy and security problems, we can not always apply the solutions to the RFID system because most of them have high-cost hardware implementation and some are inconvenient to customers.

Blocker tag is a solution for privacy protection. It is based on the anti-collision algorithm of Radio Frequency Identification technology. This should be an efficient method to protect user privacy. However, if this method is used in malicious way, the inventory of the RFID reader might be stopped, and people may carry something out without accounting. This could be a serious problem on RFID application for world-wide usage. In this work we proposed a new scheme to slove the security problem raised by blocker tag.

Keywords: anti-collision, blocker tag, RFID, privacy, inventory

本論文能夠順利地完成，不是單單只倚靠個人的辛苦以及努力，而是要 歸功於許多人的指導、幫助。在此，希望以我最誠摯的心意，向你們說 聲「感謝」。

首先感謝指導教授蔡文能老師，由於他不吝於分享其豐富的經驗與 知識，讓我學會以多元的視野去看事情、做研究。 並感謝蔡宗易學長對於本論文之指正與建議。

我亦非常感謝研究室的許多伙伴們：安勝幫我繪製示意圖；彥寧、偉民、和昱華在 口試時所給予的協助。並在參加論文比賽的時候給予我許多幫忙。

最後感謝我的好朋友們： 感謝你們在我疲倦的時候給我動力，感謝昇譽常常陪我吃飯聊天。 也謝謝彥廷常常對我說加油。感謝立文因爲我在準備口試而幫我負擔一些工作。 而孟穎也常常關心我，幫我打氣。 感謝一直在支持我的好朋友們。

Chapter 1

Introduction

An RFID tag consists of a small circuit with antenna. It transmits a unique serial number for a distance of several meters. The tag replies to the reader with query response. In figure 1.1, the reader will know its product ID to keep inventory or accounting. Low-cost tag can be read and updated information without physical contact.

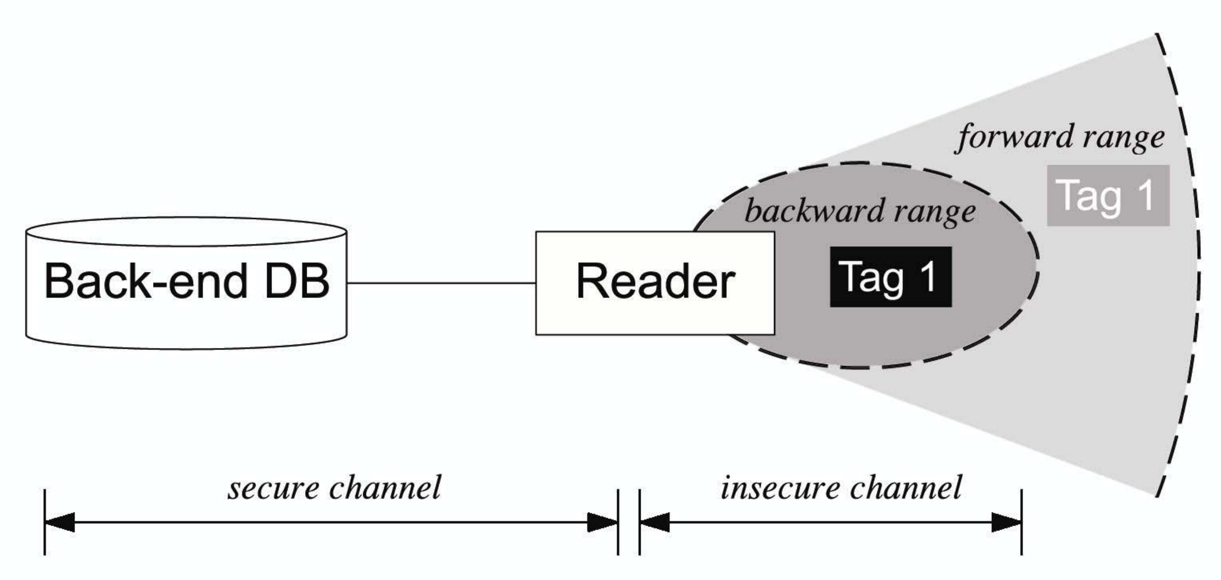


Figure 1.1: Reader reads tags without physical contact.

Therefore, the RFID system has become popular in modern application.[1, 12] Correspondingly, the privacy issue is important in real world usage of RFID. For example, in a dark corner, a robber may use RFID reader to scan the RFID tag on your body to identify your sex. In another case, your records of illness will reveal in the same way by scanning your gallipot. How to hide your RFID tag to protect your privacy is an important issue.

Because of the low-cost implementation, a malicious user is easy to get your privacy information from your packet. Base on this problem, there are many articles and researchre discussing over the privacy issue. They both intend to solve privacy problem and keep the convenience of the tag for usage.

According to the passive UHF chip we studied, it is a challenge to protect privacy. Since computing power is limited, a complex algorithm will not be applied. In RFID Class 1 Gen 2, only two functions can be used: `XOR` and `random number generator`. It is important to design an efficient algorithm on the platform.

Some researches are based on EPCglobal Standards, they try to find a solution without additional hardware implementation. Others do a little modification to the original scheme, similar to hash function, They try to solve this problem better with a slight modification.

1.1 Motivation

RSA Lab[6] proposes blocker tag scheme which doesn't need addition hardware to protect the RFID tag from read. However, people can also use this scheme to avoid the products from being accounted. RSA blocker tag was proposed only for RFID Class 1 Gen 1. We will discuss the blocker tag based on RFID Class 1 Gen 2. Unlike RSA blocker tag suffers from security problem, we propose both blocker tag scheme and detection scheme for RFID Class 1 Gen 2. The main purpose of our research is to design a new methed that can be used to protect user privacy while we can also defect it if it is used in malicious way.

1.2 Detect The Existence of Blocker Tag

The main difference between normal tag and blocker tag is collision situation. A blocker tag will echo its RN16 to block normal Class 1 Gen 2 tags. Once the blocking occurs, the reader will receive a collision signal. Collision is the main point of blocker tag.

Figure 1.2: Blocker Tag

We know that collision rate(which is the ratio of collisions over query) grows with increasing number of tag. The collision rate is not always in a fixed rage and will vary with the number of tag. We can not detect the existence of blocker tag by only using collision rates except we already knew how many tags there are.

Another feature is number of ACK. A smart blocker tag will echo its RN16 to reader to block the normal tag. But blocker tag don't know what time slot will normal tags echo, so it must echo every time. The Q algorithm adjust number of time slot to avoid collision. In our observe, Q algorithm will keep the ratio between number of ACK and number of query around 0.35. As our observe , every 100 times of query will get 50 times of ACK at most in average. If a blocker tag join into the inventory progress, the ratio will more than 0.5. We will use this condition to detect the existence of blocker tag.

Chapter 2

Background and Related Work

The main problem of killing the tag from stakeholder is that it will disable it from future merging service for customer. And thus the kill command of Class 1 Gen 2 can not be used to solve privacy issues. For example, your home refrigerator might be connected with the Internet in the future service. It can read the RFID tags from your milk box and look up the product information over Internet. It can deliver warning about expiration date of your milk by e-mail or display on the panel.

There are two privacy problems for the RFID system.[8] One is leaking personal information. In an RFID standard Class 1 Gen 2 system, anyone can read without restriction and the possessor is unaware. Another is tracking of consumer's spending history and whereabouts. Since each tag ID is unique, we can trace a person's movement by the item tagged with the RFID tag on his body. These two threats come from basic problems of RFID system.[11, 4] Anyone can read the sensitive data of tag without permission. There are four approaches to solve the problem we mentioned above.

2.1 Kill Tag

Kill RFID tags(which is actually done bye the "kill command") is the most straight way to protect user privacy. Once a tag being killed,it would never wake up again.

Auto-ID Center suggests that a tag should be killed after purechase of the tagged product. With their proposed tag design, a tag can be killed by sending it a special “kill” command with correct suicide code. The memory bank which stores kill password is shown in figure 2.1

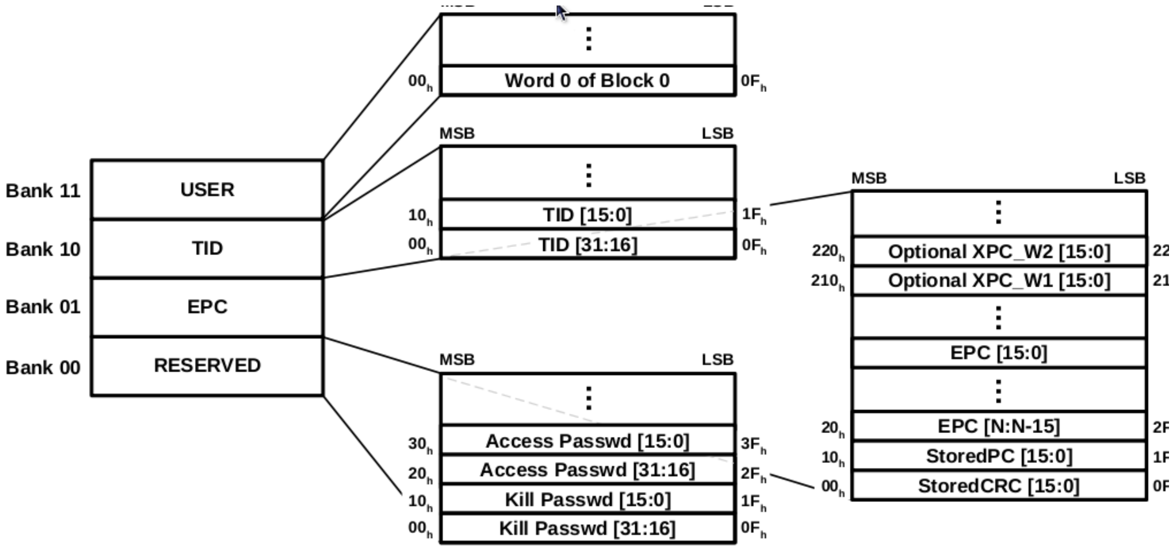


Figure 2.1: Kill password which store in memory bank.

For example, RFID tags can be used in a market to account the shelf stock. In order to protect user privacy, clerks would “kill” the tags after purchase. Clerks can "kill" the tags after purchase to protect their privacy. But the "kill" commands are not always desirable for privacy enforcement in many situation. Consumers may wish RFID tags to remain operative for many other innovative application.

For example, a Prada store in New York tracks the RFID tags of items held by customers in order to display related accessories on nearby screens. Other examples of RFID tag application,such as ordinary user usr RFID in effortless physical access control and wireless payment cards.

A powerful and low cost technology for RFID tags will inevitably be used in numerous applications,most of them are incogitable now. Most of these applications will require a living tags, not a dead one, while in the consumer's possession, and thus cannot be killed upon purchase. Here are a few suggestive of such applications:

- Stores may need products to have tags scannable even if the products are returned as defective.
- In recycling pureposes,products may need to be scanned so they may be categorized.
- When a product is returned,stores can confirm purchase with embedded RFID tags.
- User may wish to have RFID tags in their business cards to facilitate scanning by recipients. Here the tag ID may be used to create a URL referring to the actual card data.
- A store may wish to embed RFID tags in store-issued coupons, for ease of scanning at the checkout counter. A store wish the store-issued coupons embedded with RFID tags for ease of scanning at the checkout counter.
- A user may wish to read his possession's tag when a recall for a specific set of products is issued.
- Collectibles such as baseball cards and CDs should have RFID tags to help owners to manage their inventory.
- A merchant want to scan consumers for marketing purposes like advertisement.
- A refrigerator or pantry shelf may be able to tell when some food or drug product has passed its expiration (“use by”) date.
- The US Postal Service may include RFID tags in postage.
- An airline ticket may contain an embedded RFID tag to allow simpler tracking of passengers within an airport.

- Businesses may include RFID tags on the invoices, coupons, and return envelopes they mail to consumers, for ease of sorting upon return.

2.2 The Faraday Cage and Active Jamming

An RFID tag may be shielded from scrutiny using what is known as the Faraday Cage—a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies). Indeed, petty thieves are already known to use foil-lined bags in retail shops to circumvent shoplifting detection mechanisms.

If high-value currency notes do indeed come supplied with active RFID tags, then it is likely that foil-lined wallets will become big sellers! At least one company already offers a Faraday-cage-based product for privacy purposes .

RFID tags will inevitably see use, however, in a vast range of objects that cannot be placed conveniently in containers, such as clothing [16], wrist-watches, and even human beings[2].

Faraday cages thus represent at best a very partial solution to consumer privacy.

Active jamming of RF signals is another, related physical means of shielding tags from view. The consumer could carry a device that actively broadcasts radio signals so as to block and/or disrupt the operation of any nearby RFID readers.

This approach may be illegal — at least if the broadcast power is too high — and is a crude, sledgehammer approach. It could cause severe disruption of all nearby RFID systems, even those in legitimate applications where privacy is not a concern.

The approach we propose in this paper is akin to "jamming," but is much more subtle in its operation, interacting cleverly with the RFID "singulation" protocol to disrupt only certain operations.

2.3 The “Smart” RFID Tag Approach

Another general approach is to make the RFID tags a little bit “smarter,” so that they provide better privacy protection mechanism, while preserving the desired active functionality. This would typically involve the use of cryptographic methods.

These approaches are exceptionally challenging to design, given the severe cost constraints on the basic RFID tag. (With a budget of five cents, there is very little to spend on additional logic gates!)

Three instances of the “smart RFID-tag” approach that have been proposed are the hash-lock method, the re-encryption method (in several forms), and silent tree-walking.

2.3.1 The “Hash-Lock” Approach.

In this approach, due to Weis et al. [18, 19], a tag may be “locked” so that it refuses to reveal its ID until it is “unlocked.” The hash-lock approach is shown in figure 2.2

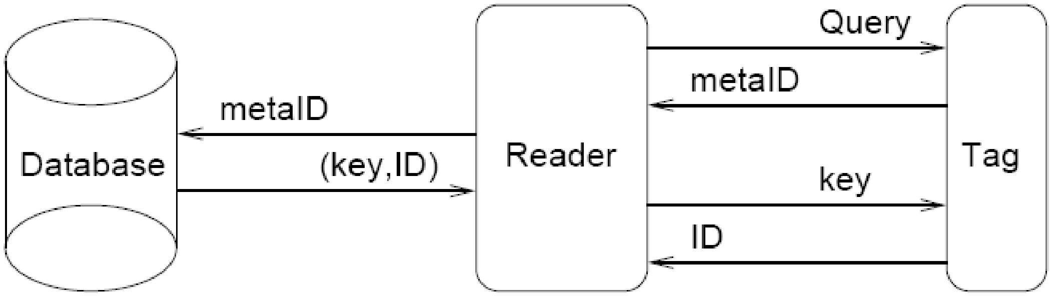


Figure 2.2: Hash Lock Approach with Back-end Server

In the simplest scenario, when the tag is locked it is given a value (or meta-ID) y, and it is only unlocked by presentation of a key or PIN value x such that y = h(x) for a standard one-way hash function h.

In the supermarket example, tags may be locked at checkout time. A consumer could provide a meta-ID y for the tags (perhaps on a loyalty card), and then transmit the unlocking PIN x via some special device (perhaps requiring physical contact) to unlock tags on returning home.

To make this approach workable, it may be necessary for a reader to query a tag to find its meta-ID, so that the reader knows which PIN to use to unlock it. But this may allow tracking of tags via their meta-IDs, defeating their whole purpose. Weis et al. show how to use randomization in the hash function computation to solve this problem.

While this is an effective approach, it seems likely that consumers will find it inconvenient to manage the lock/unlock patterns and associated PINs of more than a small collection of tags. In addition, it is possible that consumers may not even be aware of which objects in their possession carry RFID tags.

2.3.2 The Re-encryption approach.

Juels and Pappu [5] address the privacy implications of RFID-tags embedded in banknotes, with a scheme where banknote tag serial numbers are encrypted with a law-enforcement public key. The resulting ciphertexts undergo periodic re-encryption to reduce the linkability of different appearances of a given tag.

Because of the severely restricted computing resources of RFID tags, they propose that re-encryption be performed by external computing agents, e.g., publicly provided privacy enhancing stations in stores. The correct behavior of such re-encryption agents may be verified when banknotes are handled in stores and banks.

The main drawback to this approach is its resource-intensive nature. While RFID tags in their scheme do not perform cryptographic operation and would not be unrealistically costly, the required infrastructure of re-encryption agents and optical verifiers would probably be burdensome. Golle et al. [3] describe a similar scheme that is more suitable for privacy-protection of RFID tags embedded in consumer goods. They use multiple public keys, thanks to a technique they call “universal re-encryption.” This is an extension of the El Gamal cryptosystem in which it is possible to re-encrypt a ciphertext without knowing the associated public key.

The Golle et al. scheme suffers from the same drawback as that of Juels and Pappu, namely the requirement for an infrastructure of re-encryption devices.

2.3.3 Silent Tree-Walking.

Weis et al. [18] correctly note that the threat posed by passive eavesdroppers is more their ability to hear the signals broadcast by the tag reader, which may be picked up many hundreds of meters away, than their ability to hear the signals of an RFID tag, which can only be picked up nearby.

This is unfortunate, since the IDs read by the standard tree-walking singulation protocol can be inferred by hearing merely the signals broadcast by the reader.

Weis et al. show how to encrypt the reader’s transmissions, so that a passive eavesdropper cannot infer the IDs being read. Apart from the fact that this does not defend against active attacks, the authors note that their proposal relies on the somewhat unrealistic assumption of a common, secret string shared among tags; this assumption can be removed, however, if the tags can generate their own random pseudo- ID’s before singulation.

We note that our selective blocking approach is compatible with this method of protecting reader transmissions from eavesdroppers.

We note that the “silent tree-walking” and “hash-lock” approaches for constructing “smart” RFID tags (and indeed almost any conceivable approach based on smart RFID tags) involve cryptographic operations on tags. Such approaches are thus unlikely to be economically practical for the near future—the RFID chips will be smart but too expensive! The straight way to protect customer privacy is to kill the tag before they are placed in the hand of customer. Kill tag means that the tag will never be active again. We can kill it with a kill command which includes a 8-bit password.[12, 13, 7]

For example, a store shall use RFID to manage and monitor their stocks. A clerk will kill the tag before the customers checkout.

2.4 Protocol Protect

DDoS attack is a common test of protocol stability. This approach attack RFID query protocol shown in figure 2.3. Blocker tag is a kind of attack in DDoS way. By attacking the reader on the protocol, the blocker tag prevents the tag from being read. When reader query for inventory in RFID Class 1 Gen 1 protocol, a blocker tag emits both '0' and '1'. On the tree traversal, the reader will find a complete tree. It takes time and gets a useless inventory list. In RFID Class 1 Gen 2, a blocker tag occupy the all slots while inventorying. In this issue no tag can be inventoried because of completely collision .

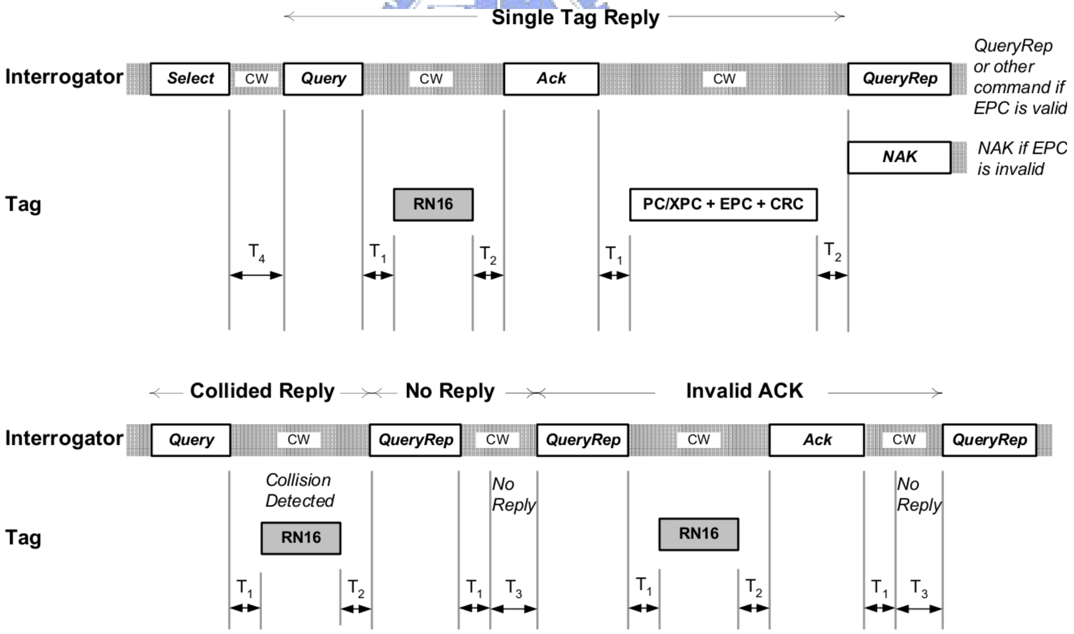


Figure 2.3: Query in RFID Class 1 Protocol

2.4.1 Blocker Tag

Our main topic is to stop blocker tag attack in world-wide usage, and how to defend attack from a blocker tag efficiently. All that we concern is as low false alarm rate and detection time as possible.

There are two kinds of RFID standard,RFID Class 1 Gen 1 and Gen 2. RFID Class 1 Gen 1 uses the tree-base algorithm to inventory tags. However it is slow in many situations; RFID Class 1 Gen 2 arises to solve this problem. RFID Class 1 Gen 2 uses the slotted-ALOHA algorithm, it is fast and can be adjusted dynamically according to collision situation. The blocker tag[6] proposed by RSA Lab was originally designed for last generation EPC Class 1 Gen 1. In this work, we discuss how to rebuild the same scenario with the Class 1 Gen 2 techonology, which uses the quite different slotted-ALOHA approach.

2.4.2 Blocker Tag in RFID Class 1 Gen 1

The blocker tag was proposed by RSA Labs. They show how to prevent the RFID reader from inventory by an abnormal tag. RFID Class 1 Gen 1 uses the tree-based algorithm as shown in figure 2.4. It can traverse the tree base on tag's product ID, by asking all tags which has prefix P. If a tag has prefix P and P's length is d, then the tag will send $d+1$'s bit of the product ID to the reader.

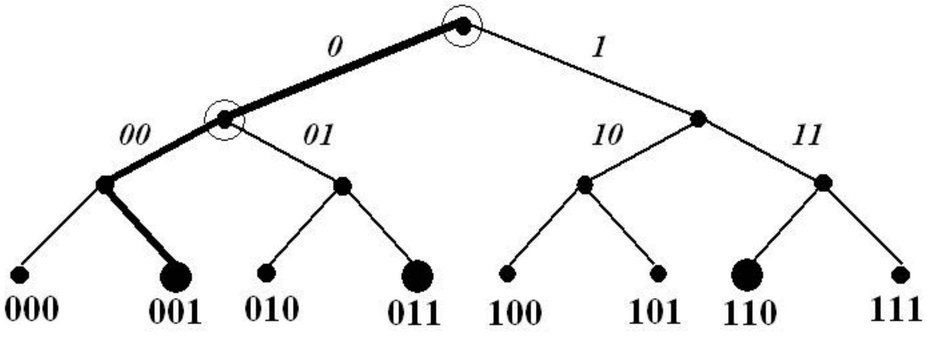


Figure 2.4: Tree-base walking of RFID Class 1 Gen 1 Protocol

By repeating the above steps, the reader can get all exist tag's ID eventually. But when a tag has two antennas and always sends both'0' and '1' to reader, the reader will do a complete tree traversal, which wastes time and causes the inventory list to be useless.

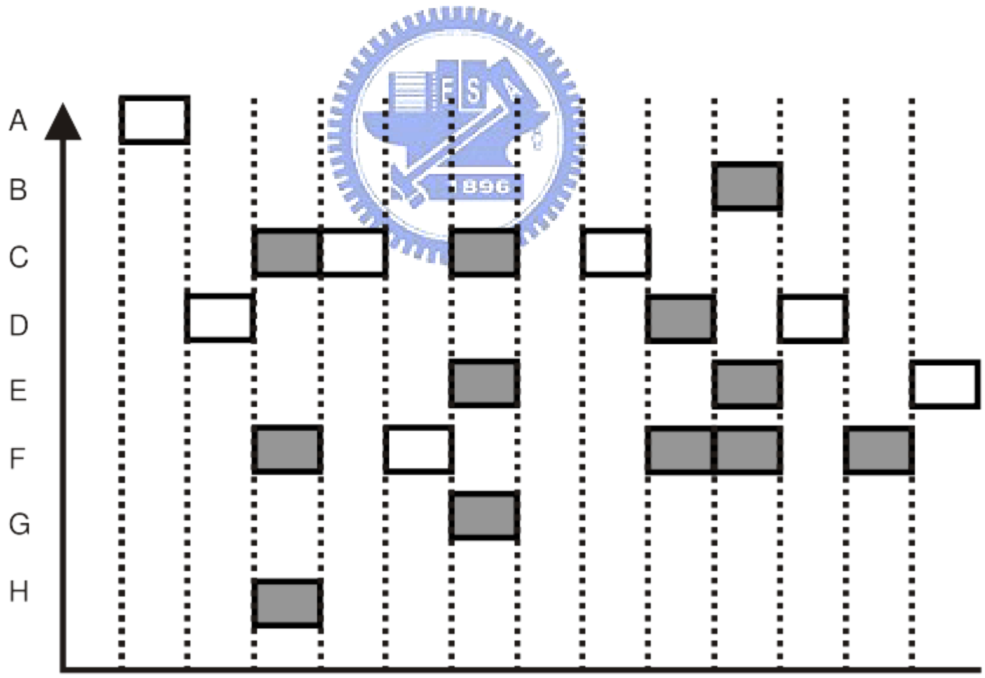
A soft blocker tag can only block a subset of ID prefix, not all of the tree traversal. This is an easy way to protect our privacy without additional hardware. But if people uses the tag in the malicious way, they can circumvent shoplifting detection.

In this case, someone can steal something from the store without checking. This must be the most serious issue on RFID accounting.

Chapter 3

Blocker Tag Detection

Blocker tag in RFID Gen 2 has many differences from Gen 1. By using the slotted-ALOHA algorithm[19, 14, 9] as shown in figure 3.1, the blocker tag can not use original ID-based scheme in jamming attack.



Slotted ALOHA protocol (shaded slots indicate collision)

Figure 3.1: Slotted ALOHA

RFID Gen 2 uses random time slots to avoid collision, we can change our idea to attack the time slot algorithm. In RFID Gen 2, the reader broadcasts query command to all tag with parameter Q. If a tag gets the command and is in ready status, it will wait for a random time T. T is a random number in the range 1 - 2^Q. When the reader detects the exist of collision, it will increase Q to lower the collision rate. We call this algorithm as adaptive-Q algorithm which is shown in figure 3.2.

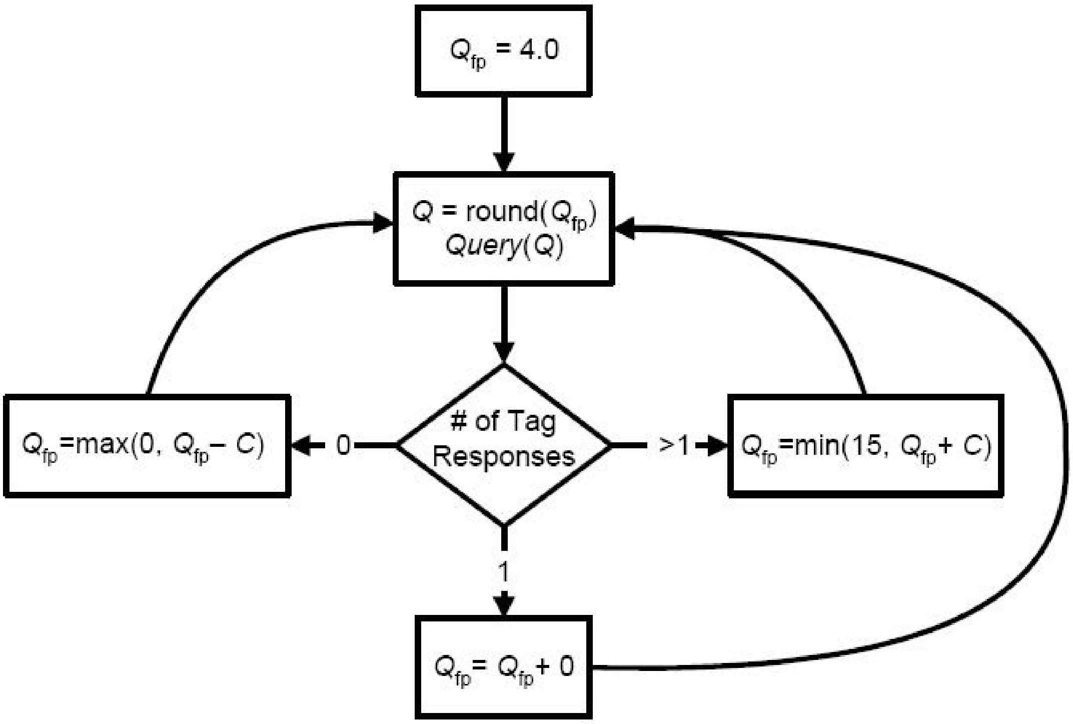


Figure 3.2: The Q algorithm

Tags can avoid collision by the nature of randomized wait. Readers can modify the parameter Q dynamically to reduce collision rate.

The blocker tag replies random product IDs every time it gets an ReqRN command, otherwise it may be detected easily through our inventory record. But blocker tag have not to reply query command every time, because partial blocking can do damage and avoid the detection.

3.1 Blocker tag Detection in RFID Class 1 Gen 1

Base on the product ID scheme, the blocker tag fabricates all the product ID of the tag. The tag responds both '0' and '1' at the same time. Because the signal send to reader at all time, we can remove it out by mathematically average.[10]

But the above method cannot be used in soft-blocker tag, because we do not know what portion that the blocker covers. In this way, we can get a sentinel tag,it's a pesudo tag that hides in the tree traversal but never echoes, in advance and we know that the ID will never reply our query. If we do a query and some tag claims that the sentinel ID exists, there must be a blocker inside. As shown in figure 3.3, we call this the sentinel scheme.

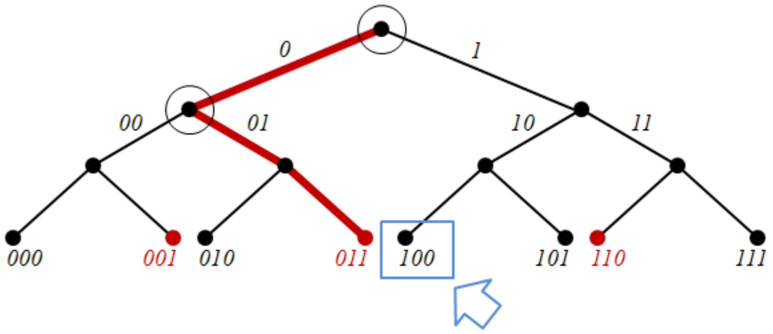


Figure 3.3: Spy tag scheme in RFID Class 1 Gen 1

In soft blocker tag scheme, a sentinel is hard to define and it is related to randomized model. We can pre-define total number scale. If the total inventory number exceeds the maximum threshold, then we can claim that there is an existing of blocker tag.

3.2 Detection Problem in RFID Class 1 Gen 2

The pervious sentinel scheme can not be applied on in RFID Gen 2, because the anti-collision algorithm in RFID Gen 2 does not use product ID to separate them all. We can detect the existence of a blocker tag by the probability scheme. If there is a blocker tag,there is high collision rate. The main idea of our approach is detecting the abnormal high collision rate.

Once a blocker tag exists, it will be useless to increase Q while querying. Choosing a threshold between Q and collision rate can detect the abnormal situation. The problem is what threshold we shall choose and how to speed up the detection time of the blocker tag.

After experiments, we know that simple fix collision rate can not be used to be a threshold as figure 3.4. Because collision rate not only changes with blocking rate but also tag number. Once tag number increases,collision rate increase too. Unless we know the number of tags already, collision rate can not stand for blocker tag's existence.

3.3 Sentienl Scheme

In another way, we can still carry on the sentinel scheme with a little modification. RFID Gen 2 uses the slotted-ALOHA algorithm to inventory. Although the algorithm does not use product ID to browse all tags, we can specify a particular product ID by select command. For example, we can use select command to select a certain product ID. Then we do a query through what we select, and we will get an expected response. If we get an echo from a mute tag, then there must be a blocker tag. But the sentinel tag is not always available, so we design another scheme.

3.4 A/Q Ratio Scheme

We define the ratio between number of ACK and number of inventoried tags as A/Q ratio. As our exeriments shown in figure 3.5,A/Q Under "Query Adjust" scheme,Q algorithm adjust A/Q ratio from 0.3 to 0.5. The maximum A/Q ratio is 1 and it means there is no collision occur. We assume that a smart blocker tag must reply "ACK" to reader if it gets correct RN16. Because a blocker tag send "ACK" too much often, it will raise A/Q ratio. If blocker tag exists,the A/Q ratio will be more than 0.5.

A blocker tag's blocking rate means how much probability of time slot it occupies. Detection and damage is a trade off. If the blocking rate is low, it is hard to detect but does little damage as the same time. The blocking rate

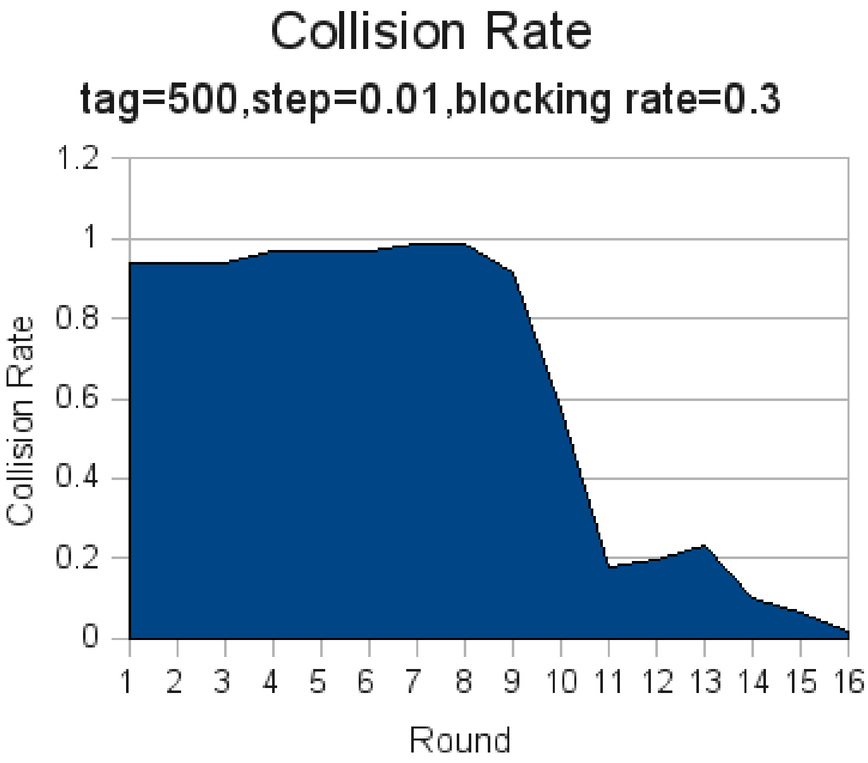


Figure 3.4: Collision rate decreases with time.

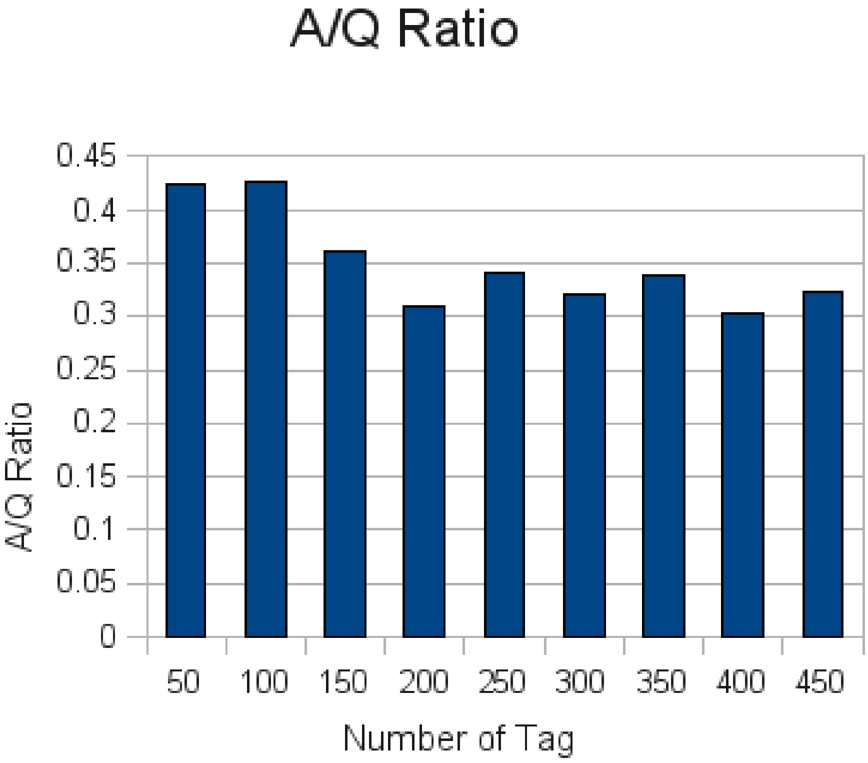


Figure 3.5: Number of ACK / Number of Query

is high, it does great damage but is easy to detect. The damage means how much time we need to inventory. 100% blocking rate will stop whole inventory.

But if the blocking rate less than 100%, the inventory must be done in a infinite time. The more blocking rate takes more time. Our job is to make a right threshold which takes reasonable time and detection rate.

3.5 Detection

Collision is an apparent phenomenon of blocker tag. Blocker tag make normal tag's echo as collision. There must be additional collision when blocker tag exists.

But we can not use collision rate to detect blocker tag. Because the collision rate comes from 1 while initial and goes to zero in the end. It's hard to make a decision to separate normal tag and blocker tag.

Because a blocker tag send "ACK" too much, it will increase A/Q ratio. By observe the A/Q ratio, we get an interest phenomenon about A/Q ratio over different number of tags. The A/Q ratio remain constant over different number of tags. The A/Q ratio in our experiment is about 0.35. The Q-Algorithm[15] show the same result with our experimental result in figure 3.6.

If blocker tag exists, the A/Q ratio will be more than 0.35. Because of the abnormal ACK from blocker tag. At the same time, blocker tag can not avoid doing those ACK. Blocker tag echo ACK in every time slot to collide with normal tag. If blocker tag stop blocking, it will not be a blocker tag.

Now we use A/Q ratio as threshold to detect the existence of blocker tag. What threshold we use is depend on what b.locking rate we want to detect. If we want to detect 80% blocking rate, we can use the target A/Q ratio 78%. In order to avoid false alarm.the threshold must much higher than 40%. Because 40% A/Q ratio is the maximum value of normal tag.

Now we use A/Q ratio as threshold to detect the existence of blocker tag. What threshold we use is depend on what blocking rate we want to detect. If

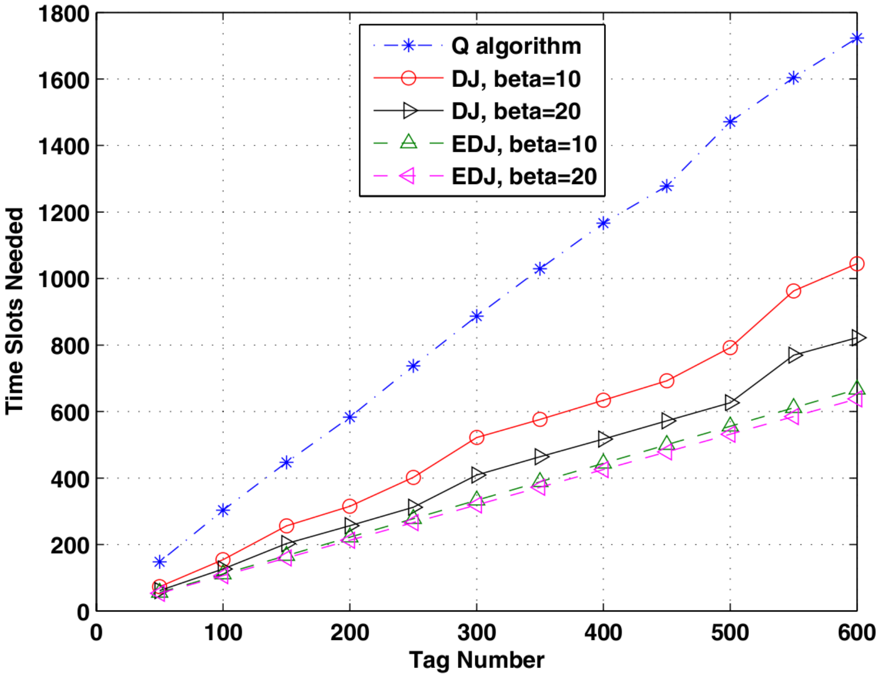


Figure 3.6: Q-Algorithm compares with DJ-Algorithm.

we want to detect 80% blocking rate, we can use the target A/Q ratio 78%. In order to avoid false alarm, the threshold must much higher than 40%. Because 40% A/Q ratio is the maximum value of normal tag.

Chapter 4

Experimental results

In order to test anti-blocker tag algorithm, we implement a simulator which follow RFID Gen 2 Protocol. RFID tags implement 7 status: Ready, Arbitrate, Reply, Acknowledged, Open, Secured, Killed. Because RFID inventory protocol involves with first 5 status, our simulator implements first 5 status only.

4.1 Assumption

A real environment of RFID system may have noise and fading. To simplify our simulation, we assume that there is an error free environment. A blocker tag in "Acknowledged" status which receives ReqRN command from the reader will reply its handle. If a blocker tag don't do so, the reader can easy detect this abnormal behavior. We define a blocker from a normal tag, but a blocker tag's slot value always equal to zero.

4.2 Environment

There are 4 variable in this simulation: initial Q, query adjust step, number of tag, blocking rate. The output is number of query which stands for performance. Initial Q is the initial value of Q in Q algorithm. According to query adjust with Q algorithm, the initial value of Q is not important. The

Q algorithm will adjust Q value dynamically. Query adjust step effects the converging speed. If the step value is too big, Q value will flip-flop. If the step value is too small, the converging speed will too slow. By our observation, the step value equal to 0.05 is reasonable. Number of tag and blocking rate are our main target to observe. If a blocker tag blocking all time slot in anti-collision algorithm, it will be detect easily because of the high slot available rate. To lower the blocking rate lower the destructive power. But to lower the blocking rate is also hard to detect.

4.3 Result

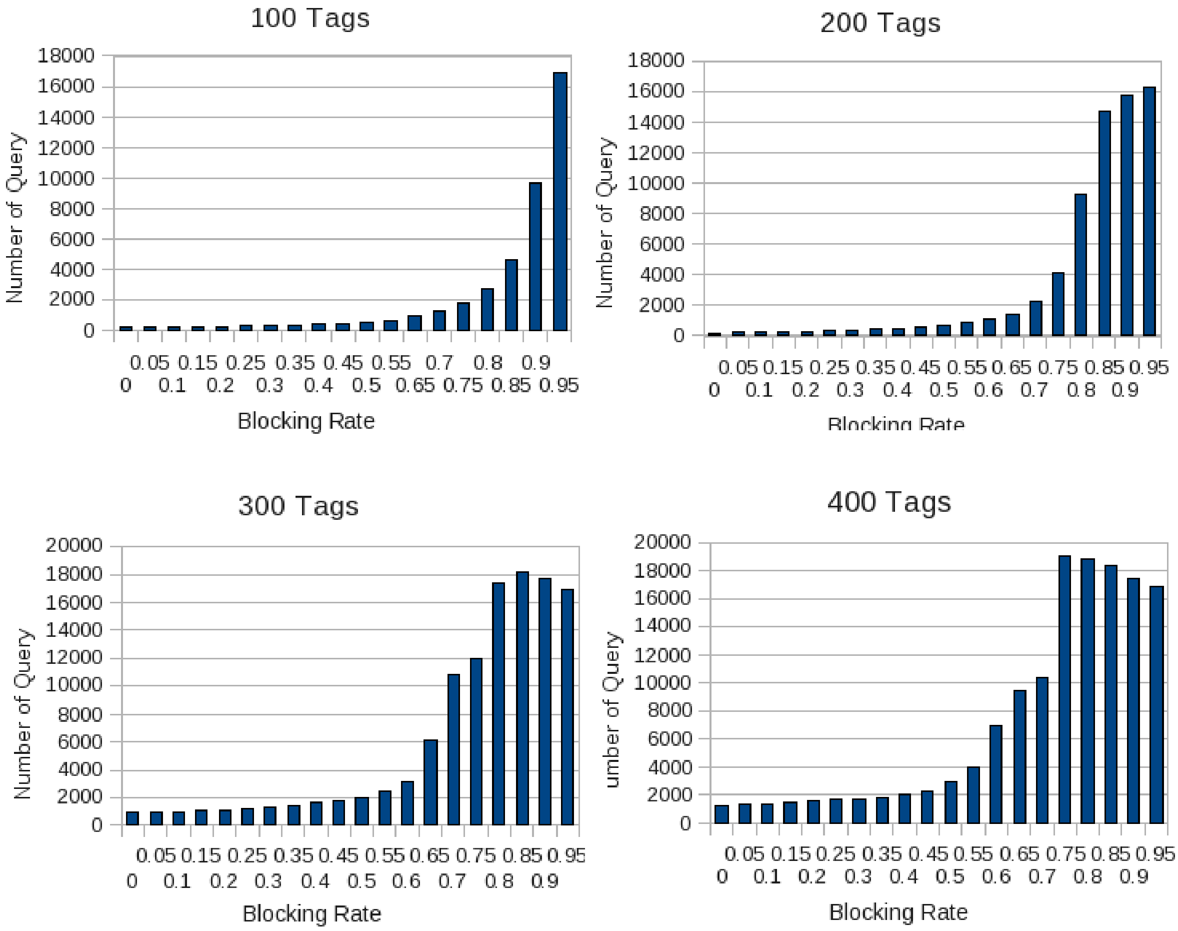


Figure 4.1: Number of Query V.S Blocking Rate

We know that number of query grows up by blocking rate. Blocker tag can be detected by observe the blocking rate. From 100 to 400 tags, we observe that number of query increases as tag number grows. It is hard to make a threshold for an unknown tag number. Because different number of tag have different number of query.

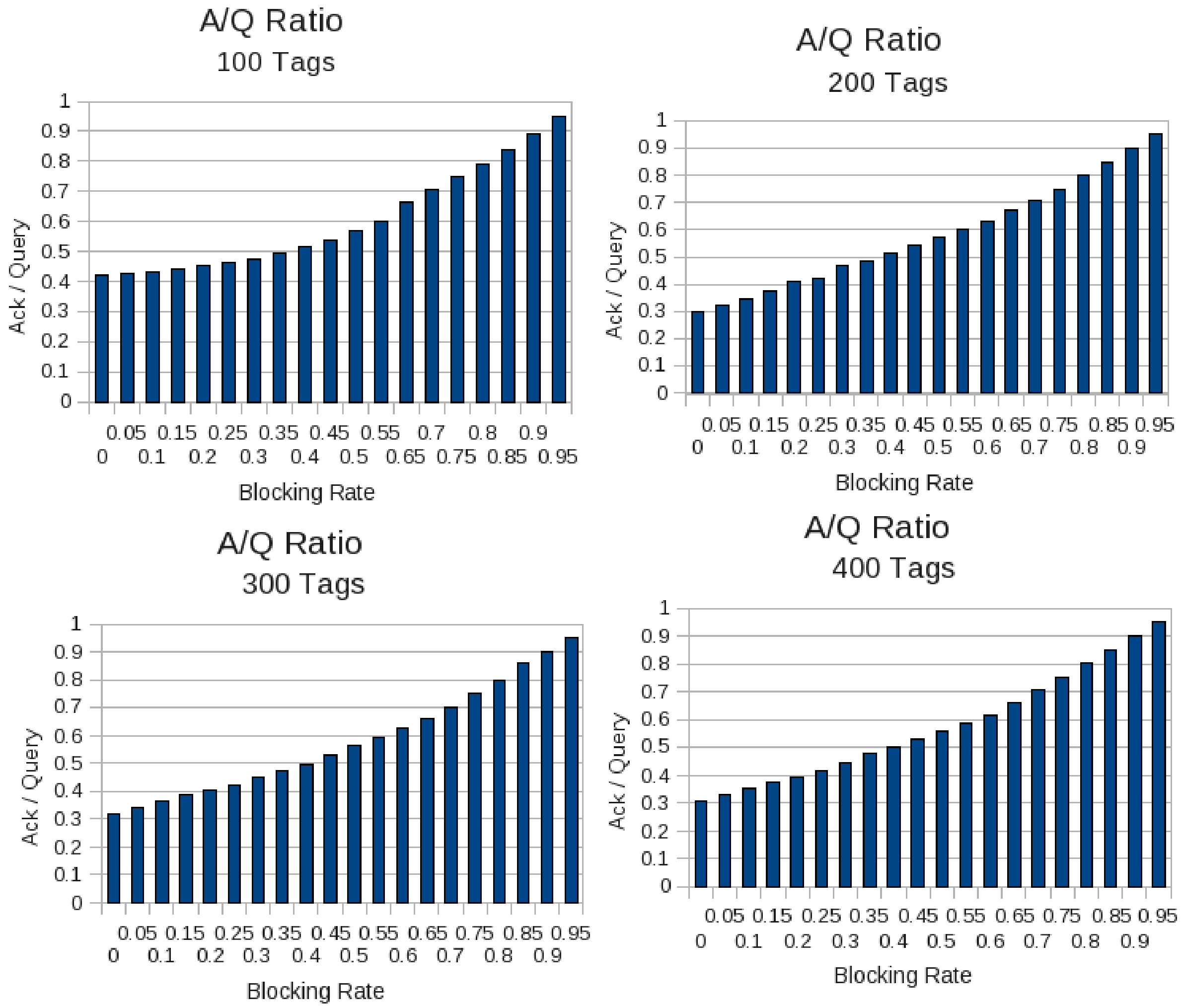


Figure 4.2: Number of Query / Number of ACK V.S Blocking Rate

In another way, we observe the ratio between number of query and ACK. In figure 4.2, the ratio between number of query and ACK is almost constant in different number of tag. Because of Q-Algorithm will adjust the A/Q ratio by number of collision and empty slot, the A/Q ratio remain constant.

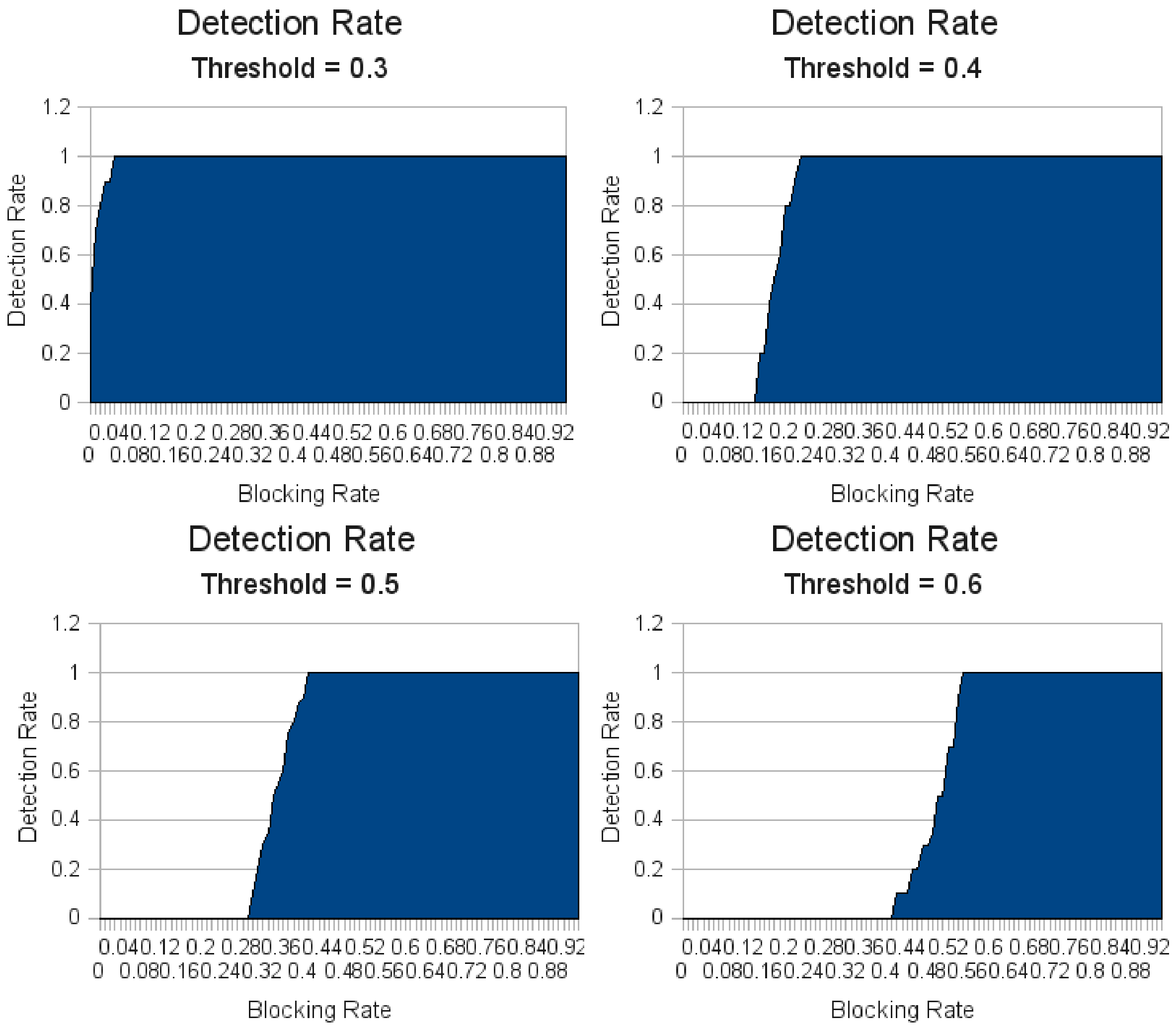
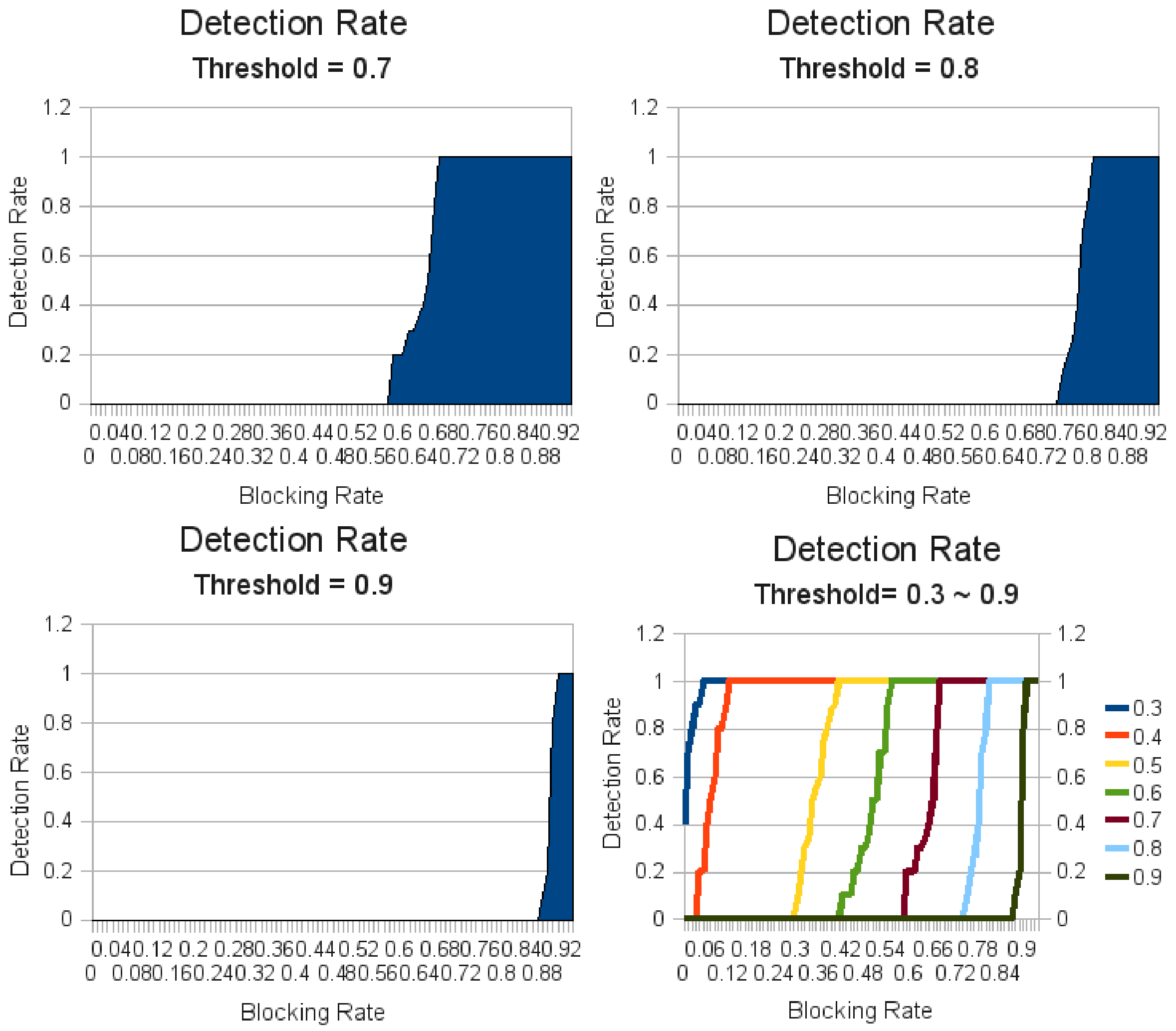


Figure 4.3: Detection Rate : 0.3 to 0.5

We design an experiment to see how threshold effects the detection rate. If the blocking rate is equal to zero, it means a normal tag and we get a non-zero detection rate. That was a false alarm happened when we detect a normal tag as blocker tag. Set the threshold of A/Q ratio from 0.3 to 0.6, at first we can watch there are false alarm in A/Q ratio equal to 0.3. But false alarm stops after increasing the A/Q ratio to 0.4.



Detection Rate

Threshold = 0.7

Detection Rate

Threshold = 0.8

Detection Rate

Threshold = 0.9

Detection Rate

Threshold= 0.3 ~ 0.9

Figure 4.4: Detection Rate : 0.6 to 0.9

When the threshold of A/Q ratio increases, we get little ability of detection. But at the same time, larger threshold means that is far away from false alarm. Besides setting threshold to 0.3, larger threshold makes no mistake in detection.

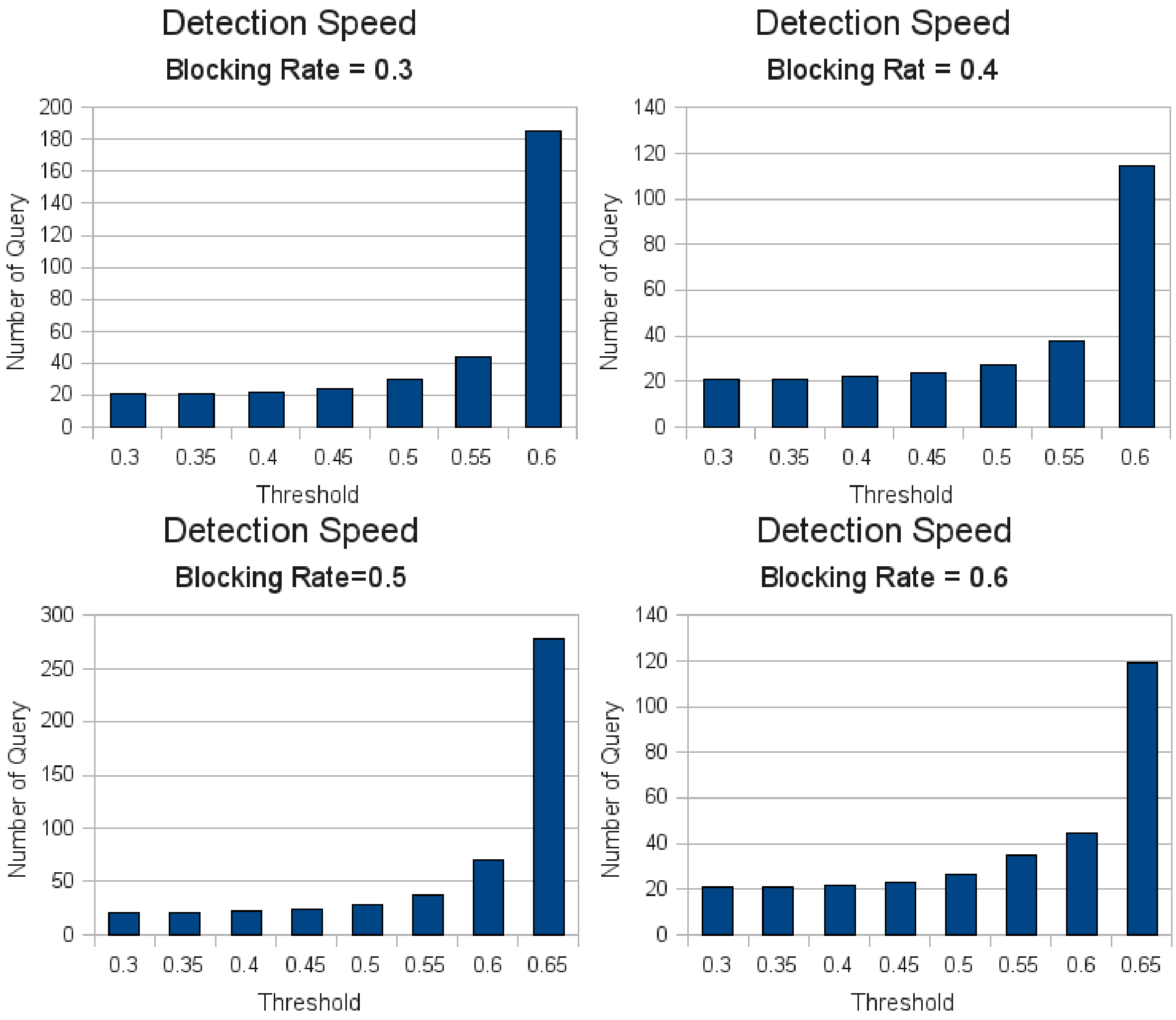


Figure 4.5: Detection Speed : 0.3 to 0.6

We want to observe how many time it takes in different threshold. Set blocking rate from 0.3 to 0.9 and observe how many time it takes. But we can not test all threshold in any blocking rate, because low blocking rate is hard to detect by large threshold. While blocking rate is equal to 0.3, we can get any detection when the threshold is larger than 0.6.

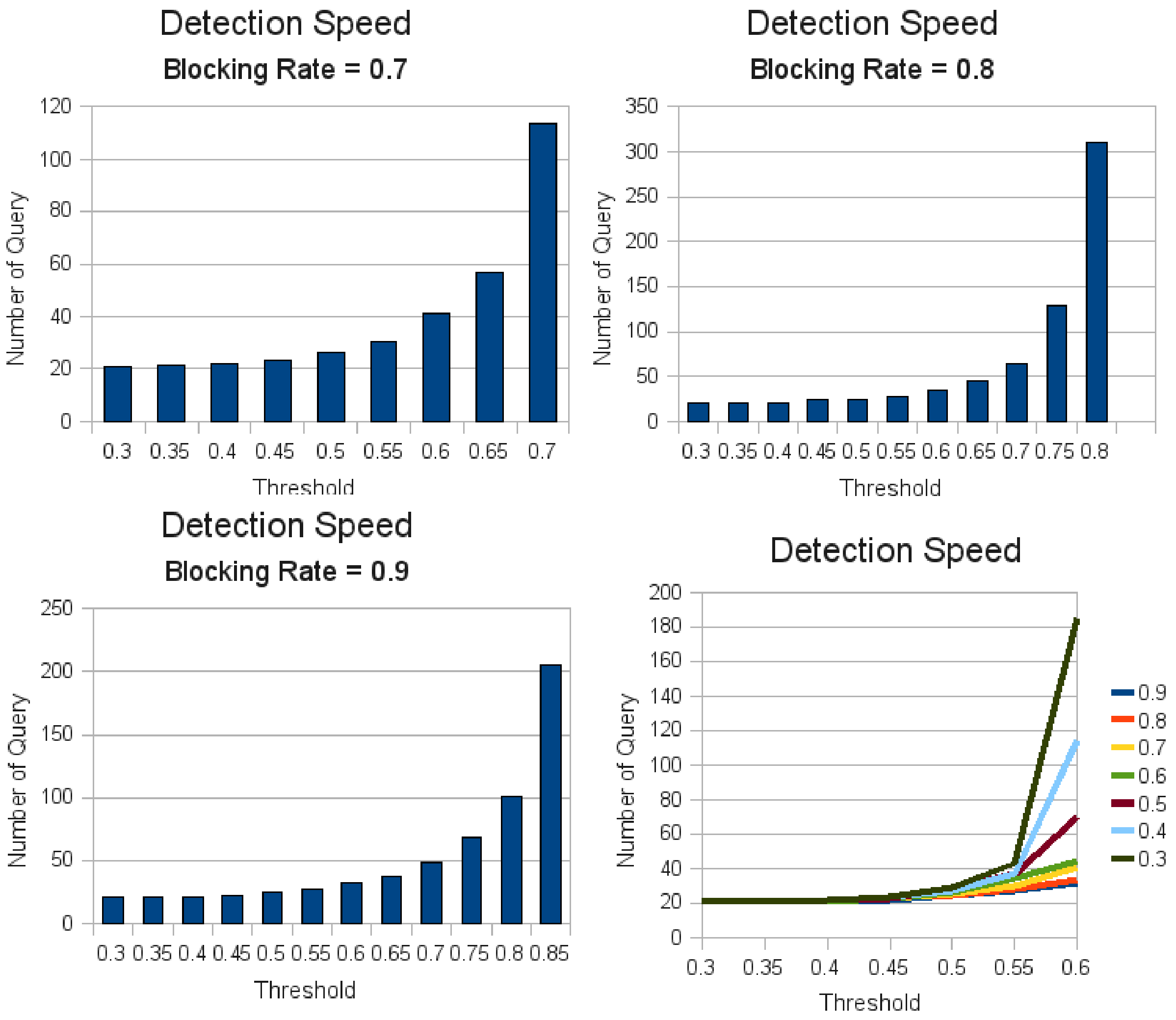


Figure 4.6: Detection Speed : 0.7 to 0.9

According to our test result, cost of time increases violently when threshold is large. If we set a large threshold, we will need more time to complete this job. Small threshold has a fast detection speed. But remember the result we discuss above, a threshold smaller than 0.3 will get false alarm. In our test, the best threshold is the A/Q ratio which is equal to 0.4. Because we increase the threshold 0.1 every step. The optimal threshold must between 0.3 and 0.4

Chapter 5

Conclusion and Future work

Obviously, we can detect a blocker tag in a range of zone. In RFID Class 1 Gen 1, we can ignore full blocker tag. But we cannot ignore the soft-blocker tag. Because we don't know the certain portion which the soft-blocker tag protects. We cannot just ignore the blocker tag or bypass its response in RFID Class 1 Gen 2 either. In some situation, people uses blocker tags to protect something while accounting. We can detect this action, and then ask the customer to remove the blocker tag or check his bag. In this way, people can use blocker to protect their item in hand but they must remove their blocker tag while accounting.

The blocker tag scheme we proposed is a complete scheme which is both for protection and detection. We design a strong blocker tag which can protect user privacy. And we design a sensitive detection algorithm to discover it. A good blocker tag can protect user privacy even if it be found by reader. A good detection algorithm can detect the existence of blocker tag even if it can not read any tag. Unlike blocker tag in Gen 1[6] which but only protect user privacy but also attack accounting. Our proposal can protect user privacy and stop shoplifting at the same time. Even if you don't use blocker as your privacy protection scheme, you still need use anti-blocker tag scheme to stop shoplifting. This anti-blocker tag scheme can provide more security while accounting.

The future work is to find a suitable threshold for different cases. Different thresholds are needed by different tag numbers. It is clear to detect the blocker existence in 1024 time slots with 100% collision rate and only ten tag existing. Maximizing the threshold will improve false alarm rate. On the other hand, maximizing the threshold harms the detection speed.

In RFID Class 1 Gen 2 system, based on the same false alarm rate,we can add sentinel to see how many thresholds are needed, to see if a sentinel really improves our scheme.

The blocker tag scheme we proposed can deal with only one blocker tag which exists in reader's access range. If there is more than one tag, A/Q ratio will not be raising by abnormal ACK from blocker tag. We can imagine that if there are two blocker tag with 100% blocking rate, there will be no ACK in the system. In order to detect two blocker tags, we can use collision rate to detect it easily.

More then two blokcer tags is just the same with two blocker tags. Because we get three event in collision detection, collision, exact one , and empty. Reader can not seperate two tags collision or three tags collision. Reader get 0, 1, 2+, which are number of total tags replied. Two or more than two is just the same. So we can use two tags to enumerate all situation.

Obviously, we can not combine detecting of one blocker tag and two blocker tags together. Because we know collision rate is meaningless in detecting one blocker tag and we want to use it in detecting two blocker tags. Unless we can distinguish one blocker tag or two blocker tags first, or we can not combine two method we mention above.

Bibliography

[1] D. M. Ewatt and M. Hayes. Gillette razors get new edge: Rfid tags. Information Week, 13 January 2003.

[2] S. Garfinkel. An rfid bill of rights. Technology Review, page 35, October 2002.

[3] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. universal re-encryption for mixnets. In submission, 2002.

[4] A. Juels. Rfid security and privacy: A research survey. IEEE Journal on Selected Areas in Communication, page 24(2), February 2006.

[5] A. Juels and R. Pappu. Squealing euros: Privacy protection in rfid-enabled banknotes. In R. Wright, editor, Financial Cryptography '03, 2003.

[6] Ari Juels, Ronald L Rivest, and Michael Szydlo. The blocker tag: Selective blocking of rfid tags for consumer privacy. Atluri, ed. 8th ACM Conference on Computer and Communications Security, In V:103--111, 2003.

[7] Günter Karjoth and Paul Moskowitz. Disabling rfid tags with visible confirmation: Clipped tags are silenced. In Workshop on Privacy in the Electronic Society — WPES, Alexandria, Virginia,USA, pages 27--30, November 2005.

[8] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Rfid privacy issues and technical challenges. Communications of the ACM, Volume 48, Issue 9:66--71, 2005.

[9] International Standards Organization. Iso/iec 15693: Identification cards - contactless integrated circuit(s) cards - vicinity cards. 2000.

[10] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. Keep on blockin’ in the free world: Personal access control for low-cost rfid tags. Lecture Notes in Computer Science, Volume 4631/2007:51--59, 2007.

[11] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. Rfid guardian: A battery-powered mobile device for rfid privacy management. Australasian Conference on Information Security and Privacy - ACISP'05, LNCS 3574, pages 184--194, July 2005.

[12] S. E. Sarma, S. A. Weis, and D. W. Engels. Radiofrequency identification systems. Workshop on Cryptographic Hardware and Embedded Systems, pages 454--469, 2002.

[13] S. E. Sarma, S. A. Weis, and D.W. Engels. Rfid systems, security and privacy implications. Technical Report MIT-AUTOID-WH-014, AutoID Center, MIT, 2002.

[14] Ronald L. Rivest Stephen A. Weis, Sanjay E.Sarma and Daiel W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. First International Conference on Security in Pervasive Computing, 2003.

[15] Jianwei Wang, Dong Wang, and Yuping Zhao. Fast anti-collision algorithms in rfid systems. International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pages 75--80, 4-9 Nov. 2007.

[16] Jianwei Wang, Dong Wang, and Yuping Zhao. Benetton undecided on use of 'smart tags'. Associated Press, 8 April 2003.

[17] R. Want. An introduction to rfid technology. IEEE Pervasive Computing, vol. 5:25--33, Jan.-Mar. 2006.

[18] S.A. Weis. Radio-frequency identification security and privacy. Master's thesis, M.I.T, June 2003.

[19] Stephen A. Weis. Security and privacy in radio-frequency identification devices. Masters Thesis. MIT, May 2003.