Security, Privacy and Efficiency in RFID Systems

by

Ehsan Vahedi

B.Sc., Electrical Engineering, K. N. T. University of Technology, Iran, 2004
M.Sc., Electrical and Computer Engineering, University of Tehran, Iran, 2008

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

The Faculty of Graduate and Postdoctoral Studies

(Electrical and Computer Engineering)

THE UNIVERSITY OF BRITISH COLUMBIA
(Vancouver)

September 2013

Abstract

Radio frequency identification (RFID) is a ubiquitous wireless technology that allows objects to be identified automatically. Using the RFID technology can simplify many applications and provide many benefits but meanwhile, the security and privacy of RFID systems should be taken into account. In this thesis, we have two goals. The first one is to improve the security and privacy in RFID systems. Our second goal is to provide accurate analytical models for the most important tag singulation schemes. We use these analytical models to evaluate and compare the efficiency of the tag singulation schemes.

First, we study the blocking attack in RFID systems and develop an analytical model for it. Using this analytical model, we propose two probabilistic blocker tag detection (P-BTD) algorithms for RFID systems that operate based on the binary tree walking and ALOHA techniques.

Then, we study the security and privacy of some recently introduced light-weight authentication protocols, and discuss their advantages and drawbacks. Based on this analysis and considering the hardware limitations of RFID tags, we propose a new authentication protocol that improves the security and privacy in RFID systems.

By taking advantage of the analytical model we proposed for the ALOHA-based P-BTD algorithm, we develop an accurate tag estimate method. Using the proposed method, we can estimate the number of tags in RFID systems accurately, and design more efficient ALOHA-based tag singulation mechanisms.

Next, we study the EPC Gen-2 protocol and its tag singulation mechanism. We model

the EPC Gen-2 protocol as an absorbing Markov chain. Using the model proposed, we derive accurate analytical expressions for the expected number of queries and the expected number of transmitted bits needed to identify all tags in the RFID system.

Finally, we study the use of the CDMA technique for RFID systems. We model the CDMA-based tag singulation procedure as an absorbing Markov chain, and derive accurate analytical expressions for the expected number of queries and the amount of transmitted data needed to identify all tags in the system. Using the analytical models developed, we compare the performance of the CDMA-based and the EPC Gen-2 tag singulation schemes.

Preface

Hereby, I declare that I am the first author and the principal contributor of this thesis. I have also benefited from the valuable comments and advice of Dr. Rabab K. Ward, Dr. Ian F. Blake, Dr. Vahid Shah-Mansouri and Dr. Vincent W.S. Wong.

The following publications describe the work completed in this thesis. In some cases, the conference papers contain materials overlapping with the journal papers.

Journal Papers Accepted/Published

- Ehsan Vahedi and Vincent W.S. Wong and Ian F. Blake and R. K. Ward, "Probabilistic Analysis and Correction of Chen's Tag Estimate Method," *IEEE Trans. on Automation Sciences and Engineering*, vol. 8, no. 3, pp. 659-663, July 2011.

- Ehsan Vahedi and Vahid Shah-Mansouri and Vincent W.S. Wong and Ian F. Blake and Rabab K. Ward, "Probabilistic Analysis of Blocking Attack in RFID Systems," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 3, pp. 803-817, September 2011.

- Ehsan Vahedi and Rabab K. Ward and Vahid Shah-Mansouri and Vincent W.S. Wong and Ian F. Blake, "On Securing RFIDs Against Blocking Attacks," *IEEE MMTC Letter*, vol. 2, no. 6, pp. 16-18, December 2011.

- Ehsan Vahedi and Rabab K. Ward and Ian F. Blake, "Performance Analysis of RFID Protocols: CDMA vs. the Standard EPC Gen2," *IEEE Trans. on Automation Sciences and Engineering*, Accepted, August 2013.

Book Chapter

- Ehsan Vahedi and Vincent W.S. Wong and Ian F. Blake, "An overview of cryptography," *Advanced Security and Privacy for RFID Technologies*, IGI Global, Chapter 6, pp. 70-100, March 2013.

Conference Papers Published

- Ehsan Vahedi and Vahid Shah-Mansouri and Vincent W.S. Wong and Ian F. Blake, "A Probabilistic Approach for Detecting Blocking Attack in RFID Systems," *IEEE ICC'10*, Cape Town, South Africa, May 2010.

- Ehsan Vahedi and Rabab K. Ward and Ian F. Blake, "Security Analysis and Complexity Comparison of Some Recent Lightweight RFID Protocols," *CISIS'11*, LNCS 6694 (Springer-Heidelberg), Malaga, Spain, June 2011.

- Ehsan Vahedi and Rabab. K. Ward and Ian F. Blake, "Analytical Modelling of RFID Generation-2 Protocol Using Absorbing Markov Chain Theorem," *IEEE Globecom'12*, Anaheim, USA, December 2012.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ACK	Acknowledgment
AES	Advanced Encryption Standard
CDMA	Code Division Multiple Access
CRC	Cyclic Redundancy Check
DFSA	Dynamic Framed Slotted ALOHA
DMV	Department of Motor Vehicles
DoS	Denial of Service
DS	Direct Sequence
ECC	Elliptic Curve Cryptography
EPC	Electronic Product Code
ETC	Electronic Toll Collection
FH	Frequency Hopping
FMC	First Markov Chain (Model)
FSA	Framed Slotted ALOHA
HF	High Frequency
HM	Hybrid Modulation
ID	Identification (Number)
ISO	International Organization for Standardization
LF	Low Frequency

MAC	Medium Access Control
NS	Non-Secret
PA	Pure ALOHA
P-BTD	Probabilistic Blocker Tag Detection
PN	Pseudo-Noise
PRNG	Pseudo-Random Number Generator
RFID	Radio Frequency Identification
RN16	Random Number (16-bit)
SHA	Secure Hash Algorithm
SMC	Second Markov Chain (Model)
SQUASH	Square Hash
TH	Time Hopping
UHF	Ultra High Frequency
ZK	Zero Knowledge

Acknowledgments

First and foremost, I would like to offer my sincerest gratitude to my supervisors, Dr. Rabab K. Ward and Dr. Ian F. Blake, for their invaluable advice, insightful guidance, and continuous patience. They have improved the quality of my research, analytical thinking and presentation skills by their constructive comments, from the early stages of my research until the very end. They have supported me and encouraged me throughout my PhD study. Honestly without them, this research would not be possible. I would like to thank them for their invaluable consideration and understanding of the conditions and problems that I was involved with as a new international student. Even in my personal life and during the hardest days, they have always been there by my side when I needed them and helped me with their invaluable advice. Briefly speaking, they have truly been more than PhD supervisors to me, and I will owe them for the rest of my life.

I would like to express my gratitude to Dr. Vincent Wong for his technical comments and advice, Dr. Robert Schober and Dr. Mehrdad Fatourechi for their invaluable help and support, and Dr. Vahid Shah-Mansouri for his constructive suggestions and guidance through out my research. I would also like to thank the members of my doctoral committee for their invaluable time and suggestions.

I am also thankful to my friends, especially Armaghan Eshaghi, Vahid Shah-Mansouri, Keivan Ronasi and Sardar Malekmohammadi for their always being supportive and accountable. I also want to thank Ahmad, Anahita, Hamidreza, Fahimeh, Peyman, Morteza, Sergio, Mohammad, Negar, Lino, Mani, Sima, Man Hon, Ali, Hamid, Di, Saloome, Babak,

Hamed, Ehsan, Tanaya, Arian, Simon, Pedram and all my other friends that definitely I cannot name them all here.

I would like to show my respect and express my gratitude to Dr. Mohsen Shiva and Dr. Caro Lucas, former faculty members of the University of Tehran and my previous mentors who are not among us anymore. Both my academic and personal life have greatly benefited by my scientific collaboration with Dr. Shiva and Dr. Lucas, and most of all, by their invaluable friendship. I will miss them for sure in the days and years to come.

Lastly, and most importantly, I feel indebted to my great family, my father Ahmad, my mother Roya, and my brothers Pouyan and Hossein for their everlasting love, support, and protectiveness not only in the past four years but also throughout my entire life. I would also like to thank Mina Irani, Mahmoud, Rosa and Reza Riazi, and Abbas Tavakkoli for always being encouraging and supportive.

I am really grateful for the opportunities I was given in Canada and appreciate the hospitality and generosity of the Canadian society. This work was supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

Dedication

With love, to my mom and dad,

and in memories of Dr. Mohsen Shiva... .

Chapter 1

Introduction

Radio frequency identification (RFID) is a ubiquitous wireless technology which allows objects to be identified automatically. This technology is expected to play an important role in various applications such as labeling products and supply chain management, object tracking, patients' monitoring in health care facilities and e-passports [8, 9, 10, 11]. There are also many other potential applications such as smart refrigerators that can recognize expired food packages and smart microwaves that know how long to cook a certain food item [12].

An RFID system consists of several RFID tags and at least one RFID reader. An RFID tag is a small electronic device with an antenna and has a unique serial identification (ID) number. An RFID reader is an electronic device which transmits and receives the radio frequency waves used to communicate with the tags.

Using RFID tags can simplify many applications and provide many benefits but at the same time, privacy of the customers should be taken into account to prevent unwanted issues which may arise from using the new technology. Many customers are currently reluctant to use RFID embedded products because of the privacy issues. On the other hand, the manufacturing costs of RFID tags should be kept as low as possible (below 5-10 cents for many applications), that itself imposes strict limitations on the hardware architecture of RFID tags. As a result, RFID tags have very limited computational capabilities and memory, and they cannot calculate sophisticated cryptographic functions. Therefore, it is crucial to develop some strategies and protocols to improve the security and privacy of

RFID systems without imposing too much computational costs to the tags. In this thesis, we study the vulnerability issues of current RFID protocols, and try to improve the security and privacy of communication between the tags and the reader(s) in RFID systems.

One of the key aspects of every RFID system is the tag identification procedure. Finding an efficient, fast and reliable tag identification procedure has recently been the focal point of many research programs. As a result, many tag identification techniques have been proposed in recent years. However, the standard EPC Generation-2 protocol has still kept its dominance over other techniques and it is widely used by industry. Although the EPC Generation-2 protocol is very efficient and literally has been accepted as the most efficient tag identification protocol, to the best of our knowledge, no accurate analytical model had been provided for it before [84]. Therefore, the only possible way to evaluate the EPC Generation-2 protocol for different applications and to compare it with other proposed tag identification techniques was simulating the whole RFID system, which is very time-consuming and more importantly, only provides approximate values for the evaluated factors. In this thesis, we propose an accurate analytical framework for the standard EPC Generation-2 protocol. Using this analytical model, the performance of the the EPC Generation-2 protocol can be evaluated accurately and compared with other proposed tag identification techniques. In the next subsections, we introduce RFID systems, discuss their security and privacy issues, explain the most popular tag identification techniques, and describe the directions of our work.

1.1 Radio Frequency Identification (RFID)

An RFID system consists of some objects with tags and at least one reader. Each tag is a small electronic device with an antenna and has a unique serial identification (ID) number. An RFID tag transmits its ID (or sometimes only a portion of it) over the wireless channel

in response to an interrogation or a query message from a reader. Commercial applications of RFID include inventory checking, supply chain management, labeling products for rapid checkout at the counter, contactless credit cards and e-passports. In addition, there are many other potential applications such as smart refrigerators and smart microwaves [12]. In both the popular press and academic circles, RFID technology has seen a swirl of attention in recent years. One important reason for this is the effort of large organizations, such as Wal-Mart, U.S. Department of Motor Vehicle (DMV), Procter and Gamble, Gillette, and the U.S. Department of Defense, to deploy RFID as a tool for automated oversight of their supply chains [12, 13, 14, 15, 16].

Advocates of RFID technology describe it as a successor to the optical barcode printed on consumer products, with two important advantages; *unique identification* and *automation* capabilities. A barcode indicates the type of object on which it is printed, while an RFID tag goes a step further. It emits a unique ID that distinguishes among many millions of identically manufactured objects. The unique identifiers in RFID tags can act as pointers to a database entries containing complete transaction histories for individual items. Moreover, being optically scanned, barcodes need direct line-of-sight contact with readers, and thus they need careful physical positioning of scanned objects. Except in the most rigorously controlled environments, barcode scanning requires human intervention. In contrast, RFID tags are readable without needing direct line-of-sight and precise positioning. RFID readers can scan tags at rates of hundreds per second [12].

The main form of a barcode-type RFID device is known as an electronic product code (EPC) tag. An organization known as EPCglobal Inc. oversees the development of the standards for these tags [8]. EPC tags cost approximately 5 U.S. cents apiece in large quantities at present. In the quest for low cost, however, EPC tags adhere to a minimalist design [12]. They carry little data in the form of on-board memory. The unique ID of

an EPC tag, known as an EPC code, includes information similar to that in an ordinary barcode, but serves also as a pointer to database records for the tag. Today, an EPC code can be up to 96 bits in length [3]. Database entries for tags, however, can have effectively an unlimited size.

RFID tags can be categorized into *passive*, *semi-passive* and *active* tags [8, 12]. Passive tags do not have an on-board power source and use backscatter modulation. In other words, their transmission power is derived from the signal of the interrogating reader. Passive tags can operate in different frequency bands. Low frequency (LF) tags operate in the 124-135 kHz band and have the nominal read range of up to 0.5 m. Animal identification is one of the widely used applications of LF tags. High frequency (HF) tags, operating at 13.56 MHz, have ranges up to a meter but typically in the order of tens of centimeters. HF tags are widely used in contactless credit cards and library tags nowadays. Ultra high frequency (UHF) tags, which operate at either 860-960 MHz (and sometimes 2.45 GHz), have a range in the order of 10 m. Some RFID tags, on the other hand, contain batteries. There are two such types; semi-passive tags, whose batteries power their circuitry when interrogated, and active tags, whose batteries power their circuitry as well as their transmission. Active tags can initiate the communication with the reader, and have read ranges of 100 m or more. Naturally, they are more expensive compared to passive tags and cost about $20 or more [12].

Different standards have been suggested so far for RFID systems such as the ISO 14443, ISO 15693, ISO 18000, ISO 18092, EPC Class-1 HF, EPC Class-0 UHF, EPC Class-1 Generation-2 UHF and NFCIP-1/ECMA 340 [8, 12]. For HF and UHF RFID systems, however, the most well-known standards are the ones introduced by the EPCglobal Inc., known as the EPC Class-1 HF and the EPC Class-1 Generation-2 UHF (briefly EPC Gen-2), respectively [17]. The EPC Class-1 HF and EPC Class-1 Gen-2 UHF have dominated

the other standards developed for passive HF and UHF tags and are widely used by industry nowadays. We study these two standards in more detail in Chapter 5.

1.2 Security and Privacy in RFID Systems

Using RFID tags can simplify many applications and provide many benefits but at the same time, the privacy of customers should be taken into account to prevent undesirable issues which may arise from using the new technology. Many customers are reluctant to use RFID embedded products because of the privacy issues. Some users are concerned that while carrying items (e.g., clothes, medicine, currency) embedded with RFID tags, they can be tracked by nearby readers. In that case, consumer privacy may be violated. In addition to tracking individuals, RFID tags may also be used to extract unauthorized critical and personal information [12]. Moreover, RFID tags may be used by some malicious organizations and dealers to sell fake RFID embedded items and forge them as valuable real items [12, 18]. Denial of service is another type of problem which can be caused by attackers to interrupt an RFID-based system [19, 20]. Moreover, some specific applications demand special considerations if the RFID technology is supposed to be used for them. As an example, Molnar and Wagner discussed the issues which should be considered for RFID-based libraries [21]. Juels and Pappu explained the security issues for using RFID technology in RFID-enabled banknotes [22]. Xiao *et al.* discussed the security concerns that need to be noted in RFID-based telemedicine systems [23]. Some noticeable works are also devoted to the security issues of RFID-based e-passports include [9, 24, 25].

In order to cope with the security issues of RFID systems, various schemes have been proposed. These solutions can be divided into two general groups; the group of solutions that use cryptography to provide the required security and privacy, and the group of solutions that use approaches other than cryptography. The cryptographic solutions for RFID

security and privacy issues can themselves be divided into two main groups; light-weight authentication protocols and complex cryptographic protocols. Most RFID researchers believe that the industry needs simple and low cost RFID tags (below 5 cents per item) with limited number of logical gates. Many approaches have been suggested which have been designed based on the light-weight authentication to address the security and privacy issues of RFID systems while keeping the computational cost and the manufacturing price of RFID tags as low as possible [4, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38]. On the other hand, some other researchers believe that it is possible (or at least feasible) to use more complex cryptographic protocols in future RFID tags. They suggest the use of public key solutions such as elliptic curve cryptography (ECC) [39, 40, 41, 42] and advanced encryption standard (AES) [43] to address the security issues of RFID systems. The public key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and the other one is public. Although the secret and public keys are different, they are mathematically linked. The public key is used to encrypt the plain-text, and the secret one is used to decrypt the cipher-text. Few approaches also exist which cannot be fitted into the cryptographic solutions. For instance, Holcomb *et al.* suggested to take advantage of the power-up static random access memory (SRAM) state as an identifying fingerprinting tool to solve the security problems of RFID tags [44]. Some researchers also proposed to use blocking, jamming and physical solutions for the RFID security and privacy issues [20, 45, 46, 47].

1.3 Tag Singulation Techniques

In an RFID system with a reader and several tags, the reader and the tags share the same wireless channel. Therefore, *tag-to-tag* collision can occur when multiple tags transmit signals simultaneously to the reader. This prevents the reader from successfully identifying

any tag. Thus, the reader and the tags need to use a technique that enables the reader to communicate with the conflicting tags one at a time. Such a technique, known as the *singulation* technique, enables the reader to talk to each tag singly. Various tag singulation techniques have been proposed in [48, 49, 50, 51, 52, 53, 54, 55, 56, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67] to prevent tag-to-tag collisions. An efficient tag singulation scheme has also been standardized recently by the EPCglobal Inc. [3]. Although many techniques have been proposed to prevent tag-to-tag collisions, most of these techniques can be categorized into three main classes; the *tree-based*, *ALOHA-based* and *code division multiple access (CDMA)-based* tag singulation techniques. The tree-based techniques provide a deterministic way to identify all tags in the system while the ALOHA-based and the CDMA-based techniques are probabilistic. In the following subsections, we introduce these three classes in more detail.

1.3.1 Tree-based Techniques

The tree-based singulation techniques have been suggested by many researchers for UHF passive tags [8, 14, 45, 57, 59]. This class of singulation techniques use a deterministic approach to identify the tags in an RFID system. We have two forms of tree-based singulation techniques; the binary tree walking and the query tree techniques. Among the above two techniques, the binary tree walking has played a more important role compared to the query tree technique in RFID applications. It was also proposed as the main anti-collision strategy used in the EPC Class-0 UHF standard. The EPC Class-0 UHF standard was developed by the Auto ID lab at MIT for passive tags operating in the 915 MHz band.

In the binary tree walking tag singulation, the reader divides the tags present at its reading range into two groups based on their IDs. The reader further divides each of these two groups into two smaller groups and continues this procedure until each group only

contains a single tag. This dividing process is continued in a group until all the tags in that group are identified by the reader. After finding all tags in a group, the reader repeats this procedure for the other group and the whole tree walking process continues until all tags in the system are successfully identified by the reader. Binary tree walking can be illustrated as a process of creating and searching a tree where a node in the tree represents a reader's query. When a reader queries the tags in its vicinity using a tree-based technique, three scenarios may happen. If only one tag replies to the reader's query, the reader can successfully identify that tag. This is called a singly replied query. If more than one tag replies to the reader's query, collision happens and the reader cannot identify the replying tags. This is called a collided query. In the third scenario, called the idle query, no tag replies to the reader's query. In the binary tree walking method, a tree is constructed when the singulation process is done. A leaf node in the tree corresponds to either a singly replied or an idle query, and an intermediate node represents a collided query. In binary tree walking, the reader transmits a query to the tags containing the prefixes of the tag IDs. Every tag within the reading range of the reader compares the prefix in the reader's query with its ID and transmits its ID to the reader if the ID has the same prefix as the one sent by the reader. In this technique, all tags in a queried group transmit their IDs while the rest of the tags remain silent and wait for the next query of the reader. The content of a query is the ID of each group. The reader repeats dividing the tags into two smaller groups until it detects a single tag and receives its ID. In this technique, the searching tree is formed based on the tag IDs. When a collision occurs, the reader makes the prefix sent to the tags one bit longer by concatenating it with 0 and 1, and repeats the query again with the concatenated prefix. For example, assume that the reader queries with the 00101101 prefix and a collision happens. This means that at least two tags exist that have the 00101101 prefix in their IDs. The reader concatenates a 0 to the prefix and queries

the tags with the prefix 001011010 again. This procedure continues until all tags in the system are identified successfully by the reader. If an idle query happens, it means there is no tag in the system with the prefix 00101101, and the reader checks the other group which has a different prefix.

The query tree singulation technique, on the other hand, uses a different trick to solve the collision problem. It takes advantage of random binary sequences generated by colliding tags for the splitting procedure. In this technique, each tag has a counter initialized to 0 at the beginning of the singulation procedure. The tag transmits its ID when the counter is 0, and remains silent when the counter is 1. Therefore, all tags transmit their IDs concurrently at the beginning of the singulation procedure. The reader then transmits a feedback to inform the tags whether or not a collision has happened. According to the reader's feedback, all the tags change their counter values. If a collision has happened, the tags which were involved in the collision (i.e., their counter value were 0 at the time of collision) randomly select new binary values for their counters. On the other hand, the tags which were not involved in the collision (i.e., their counter value was 1 when collision happened) change their counter value to 0. When the reader's feedback indicates no collision, all tags toggle their counter values. The tags which have been successfully identified by the reader during the previous queries become silent and do not transmit any signal until the ongoing singulation procedure is terminated. The reader has a counter as well, which is used to terminate the singulation procedure. It initializes the counter value to 0 at the beginning of the singulation procedure. After each query, if a tag collision happens, the reader adds 1 to its counter value, otherwise, it decreases its counter value by 1. When the counter value becomes negative (<0) the reader terminates the singulation procedure.

Although the query tree method is very similar to the binary tree walking technique

in terms of the efficiency of identifying the tag IDs in the system, the binary tree walking method has been the dominant singulation technique in the class of tree-based singulation techniques. It has also been suggested as the anti-collision technique by the EPC Class-0 standard. Therefore, we are more concerned about the binary tree walking technique and study it in more detail in Chapter 2.

1.3.2 ALOHA-based Techniques

In RFID literature, ALOHA-based tag singulation techniques are also known as the *probabilistic* anti-collision schemes. The reason is that when the reader queries the tags present in its vicinity, each tag ID can be successfully detected by a probability less than one. In the ALOHA-based protocols, the communication channel is divided into time intervals called *frames*, and each frame consists of a number of *time slots* [8]. The duration of each time slot is equal to the time needed for transmitting a tag ID [68]. At the beginning of the singulation procedure, the reader sends a query message containing the length of the frame (or equivalently, the number of time slots in that frame) available to all tags in the system and waits for them to reply and send their tag IDs during these time slots. Each tag randomly selects a time slot, and transmits its ID during that slot. When all tags transmit their IDs, three scenario may happen for each time slot in the frame. If a time slot is not selected by any tag, it is called an *empty* slot and contains no information. The reader can successfully read the content (tag ID) of a time slot if one and only one tag selects that slot. This kind of time slot is called a *singly occupied* slot. Finally, if a time slot is selected by more than one tag, it is called a *collided* time slot and its information cannot be used by the reader. After each query, the tags that were successfully identified become silent, and the tags which were involved in collisions continue to select a time slot at random and send their IDs during the next queries. This singulation technique is called

framed slotted ALOHA[53]. Framed slotted ALOHA has been used as the main singulation technique for the LF RFID systems. A special form of the framed slotted ALOHA has also been suggested by the EPC Class-1 HF and the EPC Class-1 Gen-2 UHF standards.

The performance of ALOHA-based protocols is highly affected by the frame size. If the number of unidentified tags in the system is much larger than the number of available time slots in a frame, too many collisions happen and very few tag IDs are detected. On the other hand, if the number of available time slots in a frame is much larger than the number of unidentified tags, too many time slots are wasted and the efficiency of the ALOHA-based singulation technique decreases. Therefore, it is very important to choose the number of available time slots in each frame wisely if we want to increase the efficiency of ALOHA-based protocols. To do this, a new class of ALOHA-based techniques have been proposed in which the length of the frames can be dynamically changed by the reader [69, 70, 71]. These techniques are referred to as *dynamic framed slotted ALOHA*. In dynamic framed slotted ALOHA, the reader changes the number of time slots dynamically based on the number of empty, single and collided time slots in the previous query. The reader decreases the number of time slots if too many slots remained empty in the previous query, and increases the number of time slots in the frame if too many collisions happened in the previous query.

Different methods have been suggested for optimizing the frame length and adjusting the number of time slots in each query. Most of the dynamic framed slotted ALOHA schemes operate based on estimating the number of tags in the RFID systems [2, 70, 72, 73, 74, 75]. Recently, a new adaptive dynamic framed slotted ALOHA technique has also been proposed and standardized by the EPCglobal Inc. for the EPC Class-1 HF and the EPC Class-1 Gen-2 UHF RFID systems [1, 3, 76]. This new technique has dominated other ALOHA-based tag singulation techniques and it is widely used by industry for different RFID applications. In this tag singulation method, the reader changes the number of time

slots at each query based on an adaptive algorithm called the Q-algorithm. In the first query, the reader provides 16 time slots to the tags (numbered from 0 to 15) and asks them to choose one of these 16 time slots at random. After doing so, only the tags that have chosen the 0 time slot are allowed to transmit their IDs and the rest of the tags are forced to remain silent and wait for the next query. If only one tag chooses the 0 time slot, the reader can successfully read its ID, but if more than one tag choose the 0 time slot, a collision happens and the reader cannot read the transmitted tag IDs. Based on the status of the 0 time slot (which can be empty, singly occupied or collided), the Q-algorithm decides whether to increase or decrease the frame length for the next query or to keep it unchanged. In this method, the number of time slots can be changed from 0 to $2^{15} - 1$ (32768 time slots in total) by the Q-algorithm based on the status of the 0 time slot. The reader continues sending queries and reading the content of the first time slot until it successfully identifies all the tags in the system. We will study the dynamic framed slotted ALOHA technique suggested by the EPC Class-1 HF and the EPC Class-1 Gen-2 UHF standards in more detail in Chapter 5. We also show how this method outperforms other singulation techniques in terms of the number of queries and the total number of transmitted bits needed to identify all tags in the system.

1.3.3 CDMA-based Techniques

The origins of CDMA are in military and navigation systems. Techniques developed to counteract intentional jamming and eavesdropping have also proved suitable for multi-user communication systems [77]. Recently, some researchers have suggested to replace the current dynamic framed slotted ALOHA technique used by the EPC Class-1 HF and the EPC Class-1 Gen-2 UHF standards with the CDMA technique [56, 60, 61, 62, 63, 64, 65, 66, 67]. In CDMA-based RFID systems, each tag is assigned a unique code sequence

called the *spreading code* (or a pool of spreading codes to choose from). Each tag uses this spreading code to encode its tag ID. The ratio of the transmitted bandwidth to the information bandwidth is called the *processing gain* of the CDMA system. By knowing all the spreading codes, the reader decodes the received information and recovers the transmitted tag ID. This is possible since the cross-correlations between the spreading codes are zero or very small. Since the bandwidth of the spreading codes are chosen to be much larger than the information-bearing signal, the CDMA process enlarges (spreads) the spectrum of the transmitted signal. Therefore, the CDMA technique is also known as a spread spectrum multiple access (SSMA) technique [78].

There are a number of modulation techniques that can be used to generate the spread spectrum signals. The most important techniques are

- *Direct sequence CDMA (DS-CDMA)*: In this technique, the infirmation-bearing signal is directly multiplied by a high chip rate spreading code.
- *Frequency hopping CDMA (FH-CDMA)*: In this technique, the carrier frequency of the infirmation-bearing signal is rapidly changed according to the spreading code.
- *Time hopping CDMA (TH-CDMA)*: In this technique, the information-bearing signal is not transmitted continuously, instead, the signal is transmitted in short bursts where the times of the bursts are decided by the spreading code.
- *Hybrid modulation CDMA (HM-CDMA)*: If two or more of the above mentioned spread spectrum techniques are used together to modulate the spread signal, it is called the hybrid modulation spread spectrum technique [77].

Since passive RFID tags are very limited in hardware structure, it is not easy to implement FH-CDMA or TH-CDMA capabilities on them without increasing the total manufacturing costs. Therefore, among the above mentioned modulation techniques, DS-CDMA

has been suggested the most for RFID systems [56, 60, 62, 63, 65, 66].

The CDMA technique provides several useful features for RFID systems such as

- *Multiple access capability*: Assuming that multiple tags transmits their IDs using the CDMA technique at the same time, the reader is still capable of distinguishing between the tags and recovering their IDs correctly if the spreading codes used by the transmitting tags have sufficiently low cross-correlation with each other. The reader correlates the received signal with the spreading codes used by the tags in the system one by one to de-spread and recover their signals [77].

- *Protecting against multi-path interference*: In the real RFID applications, there might be more than one path between the transmitting tag and the reader (for example in a large warehouse with thousands of RFID embedded merchandises). Therefore, multiple copies of the transmitted signal might be received by the reader due to reflections and refractions. The received signals have different amplitudes, phases, delays and arrival angles. Adding these signals by the reader can be constructive at some frequencies and destructive at some other frequencies, which results in a dispersed signal in the time domain. The CDMA technique can decrease the issues that arise from multi-path interferences and improve the performance of the system [77, 78].

- *Increasing the privacy*: Using the CDMA technique, the transmitted signals can be de-spread and the tag IDs can be read only if the spreading codes are known. This feature increases the privacy of the RFID system by preventing random eavesdroppers and illegitimate readers from identifying the tags in the system [77].

- *Interference reduction*: Assuming that there exists a narrow-band interfering signal in the environment, the cross-correlation of the spreading codes with the narrow-

band interference in the reader spreads the power of the interference, which results in reducing the interfering power in the information band-width, and makes it easier for the reader to recover the tag IDs [77].

Among the above mentioned advantages of using the CDMA technique, its multiple access capability is the most desired one for RFID systems. Using this idea, it has been suggested to provide several spreading codes for the tags in an RFID system. The tags use these codes to spread (encode) their IDs, and then send their coded IDs to the reader. Using the CDMA technique, multiple tags can be simultaneously read in each query and thus the number of collisions is reduced.

Although using the CDMA technique can reduce the number of collisions and increase the number of identified tags at each query, the assumption that it speeds-up the whole tag identification procedure may not necessarily be true. In Chapter 6, we will study the use of the CDMA technique for RFID systems in more detail and investigate the efficiency of the tag identification procedure using the CDMA technique.

1.4 Contributions and Results

This thesis aims to cover two important and challenging aspects of RFID systems. The first area is the security and privacy in RFID systems, and the second one is the efficiency of RFID protocols. In the first half of the thesis, we focus on security and privacy issues of RFID systems. In the second half of the thesis, we focus on analytical modeling and performance evaluation of the state of the art tag singulation schemes. Chapters 2 and 3 address the security and privacy in RFID systems, and Chapters 4 to 6 address the analytical modeling and performance evaluation of the main tag identification schemes. The contributions of this thesis are as follows.

- We first study the blocking attack against RFID systems operating based on the binary tree walking tag singulation mechanism. Using blocker tags was originally suggested as a solution for the privacy issues of RFID systems. A blocker tag can simulate all or a portion of the tag IDs in the system and avoid undesired interrogations. However, it was revealed later that blocker tags can also be used by malicious attackers to interrupt or mislead the normal operation of RFID systems in large chain stores and warehouses. This attack, called the blocking attack, is very hard to detect automatically in large RFID systems with thousands of tags. We mathematically model the blocker attack for RFID systems that operate based on the binary tree walking singulation mechanism. Using the developed analytical framework, we propose a probabilistic blocker tag detection (P-BTD) algorithm to detect the presence of an attacker in RFID systems operating based on the binary tree walking mechanism. The proposed P-BTD algorithm can detect the existence of a blocker tag using the information extracted from the interrogations performed by the reader. Simulation results show that the proposed algorithm has a better performance than the threshold-based detection algorithm in terms of the number of required interrogations. We also study the blocking attack against RFID systems operating based on the ALOHA tag singulation mechanism. Same as RFID systems which use the binary tree walking for tag singulation, ALOHA-based RFID systems are also vulnerable to the blocking attack. An attacker may disrupt ALOHA-based RFID systems by sending fake IDs to the randomly selected time slots in each frame. The blocker causes the reader to detect some fake tags by sending some fake IDs to the slots which would have remained empty in a normal (unattacked) system. Moreover, the blocking attack reduces the efficiency of the tag identification procedure in ALOHA-based RFID systems drastically. Based on the above, we need to find an efficient way

to make sure that there is no attacker in the system and to prevent the reader from being involved in a loop of endless (or useless) interrogations. We mathematically model the ALOHA-based RFID systems and find the probabilities that the reader observes a specific frame structure in the presence and absence of a blocker tag. Using the analytical framework developed, we propose a probabilistic blocker tag detection (P-BTD) algorithm for ALOHA-based RFID systems. Simulation results show that our proposed algorithm has a better performance compared to the threshold-based detection algorithm in terms of the number of required interrogations. This work has been published in [20, 79, 80].

- We consider the use of light-weight authentication protocols for increasing the security and privacy of RFID systems. Using the light-weight authentication has the advantage of keeping the computational demand and the price of RFID tags very low while increasing the security and privacy in RFID systems. For this reason, light-weight authentication protocols have been of interest to both industry and academia. We perform the security analysis of the standard EPC Gen-2 protocol. We also perform the security analysis of five other light-weight authentication protocols proposed in [4, 5, 6, 7], and show how they can be broken by some simple tricks. We then propose a new light-weight authentication protocol that takes the hardware limitations and the manufacturing costs of RFID tags into consideration. The security of the proposed protocol and its complexity are compared with [4, 5, 6, 7]. We show that our proposed method improves the level of security and privacy by paying attention to the vulnerabilities of the protocols proposed in [4, 5, 6, 7]. Part of this work has been published in [81] and the rest has been submitted to [82].

- We propose a new probabilistic tag estimation method for ALOHA-based RFID systems. For many RFID applications, we need to know or calculate the number of tags

present in the RFID system at any time. Many tag estimation methods have been proposed to calculate the number of tags in the system. In [2], a probabilistic tag estimation method was proposed for ALOHA-based RFID systems. In this method, the reader estimates the number of remaining tags in the RFID system after each interrogation based on *a posteriori* probability, and uses this estimated number to determine the number of required time slots for the next interrogation. This approach can improve the performance of the ALOHA-based anti-collision algorithms. However, there exists a mathematical error in the probabilistic modeling of the problem. We address this problem and provide the correct probabilistic model and the correct tag estimation method for ALOHA-based RFID systems. This work has been published in [83].

- We investigate the standard EPC Gen-2 protocol and model it as an absorbing Markov chain. We formulate the proposed model and derive the expected number of queries required by the EPC Gen-2 protocol to identify all tags in an RFID system. We also derive the expected number of transmitted bits for the EPC Gen-2 protocol. These formulae allow us to provide a measure of the speed of the EPC Gen-2 protocol in identifying all tags in the system and the amount of data that should be transferred during this process. Moreover, the proposed model enables us to compare the performance of the EPC Gen-2 protocol with other schemes using the accurate formulation provided. Extensive simulations validate and confirm the accuracy of our proposed analytical model. Without this model, one has to run simulations and average the results to obtain the expected number of required queries and the expected number of transmitted bits. Using the analytical formulation provided by this model, there is no need to rely on simulations for studying the behavior of the EPC Gen-2 protocol, i.e., we are able to calculate the number of required queries and

the number of transmitted bits directly. Our proposed analytical model is also useful in studying and comparing other RFID protocols, and in deploying better protocols for RFID systems. Part of this work has been published in [84] and the rest has been submitted to [85].

- We investigate the CDMA-based RFID systems and model them as an absorbing Markov chain. Recently, some researchers have suggested to replace the dynamic framed slotted ALOHA technique used in the standard EPC Gen-2 protocol with the CDMA technique to reduce the number of collisions that happen and to improve the tag identification procedure. We model the CDMA-based tag identification process as an absorbing Markov chain, and derive the analytical formulae for the average number of queries required and the total transmitted data needed to identify all tags in an RFID system using the CDMA technique. Taking advantage of the proposed Markov chain and the one we proposed before for the standard EPC Gen-2 protocol, we compare the two tag identification protocols and show that the standard EPC Gen-2 protocol outperforms the CDMA-based scheme in terms of the total transmitted data and the average time needed to identify all tags in the system. This work has been submitted to [86].

1.5 Thesis Organization

The rest of the thesis is organized as follows. In Chapter 2, we study the blocking attack in RFID systems that operate based on the binary tree walking tag singulation mechanism. We develop an analytical model for the blocking attack against the binary tree walking tag singulation mechanism. Using this analytical model, we propose a probabilistic blocker tag detection algorithm (P-BTD) to detect the presence of an attacker in this type of RFID

systems. In the next step, we focus on RFID systems that operate based on the ALOHA tag singulation mechanism and study the blocking attack against this type of RFID systems. We develop an analytical model for the blocking attack against the ALOHA tag singulation mechanism. Using this analytical model, we propose a probabilistic blocker tag detection algorithm (P-BTD) to detect the presence of an attacker in ALOHA-based RFID systems. In Chapter 3, we investigate the security and privacy issues of the standard EPC Gen-2 protocol, and study the use of light-weight authentication protocols for increasing the security and privacy in RFID systems. After investigating the EPC Gen-2 protocol, we perform a security analysis of five light-weight authentication protocols suggested in [4, 5, 6, 7] and show their vulnerabilities. Using this security analysis, we propose a new light-weight authentication protocol which improves the level of the security and privacy in RFID systems and at the same time considers and complies with the hardware limitations of passive RFID tags. In Chapter 4, we study the probabilistic tag estimation method proposed in [2] for ALOHA-based RFID systems. In this method, the reader estimates the number of RFID tags in the system after each interrogation based on *a posteriori* probability and uses this estimated number to determine the number of required time slots for the next interrogation. We show that there exists an analytical error in the probabilistic modeling of [2]. We address this problem and provide the correct probabilistic model and the correct tag estimation method for ALOHA-based RFID systems. In Chapter 5, we study the Q-algorithm and the tag singulation protocol used in the EPC Gen-2 standard. We model the tag singulation protocol used in the EPC Gen-2 standard as an absorbing Markov chain. Using this Markov model, we derive the analytical formulas for the expected number of queries and the expected number of transmitted bits needed to identify all tags in an RFID system. Extensive simulations validate and confirm the accuracy of our proposed analytical model. In Chapter 6, we study the use of the CDMA technique for RFID

systems. The CDMA technique has been suggested by many researchers in recent years to increase the efficiency of the tag singulation procedure. We model the CDMA-based tag singulation protocol as an absorbing Markov chain. Based on this Markov model, we derive the analytical formulae for the expected number of queries and the total transmitted data needed to identify all tags in a CDMA-based RFID system. Using the analytical formulae in Chapters 5 and 6, we compare the efficiency of the EPC Gen-2 and the CDMA-based tag singulation protocols, and show that using the CDMA technique does not necessarily improve the efficiency of the tag singulation process. Finally, Chapter 7 contains discussion of the main results, conclusions, and suggesting future research directions. Each of the main chapters in this thesis is self-contained and included in separate journal articles or conference papers. The notations are defined separately for each chapter. A review of the related work is given for each chapter accordingly.

Chapter 2

Probabilistic Analysis of Blocking Attack in RFID Systems

2.1 Introduction

For pervasive deployment of RFID systems, one issue which causes the public concern is privacy. Some customers are concerned about being tracked by other readers when carrying items (such as clothes, medicine or currency) embedded with RFID tags. In addition to tracking individuals, RFID tags may also be used to extract personal information such as the type of clothes somebody wears, the specific brands that an individual is interested in, or some medical information about the patient carrying an RFID-embedded container of medicine [12]. RFID tags may also be used by some malicious organizations or dealers that sell illegally copied items (embedded with fake RFID tags) and forge them as valuable items [12, 18]. Denial of service is another type of problem which can be caused by attackers whose aim is to disrupt an RFID-based system [19, 45, 79]. Moreover, some specific RFID applications demand specific considerations. As an example, Molnar and Wagner discussed the issues that should be considered for RFID-based libraries [21]. Juels and Pappu explained the security issues concerning the use of RFID technology in RFID-enabled banknotes [22]. Xiao *et al.* discussed the security concerns of RFID-based telemedicine systems [23]. Ma *et al.* studied the security issues of RFID-based toll systems [15]. Some noticeable work has also been devoted to security issues of RFID-based

e-passports [9, 24, 25].

In order to cope with security issues in RFID systems, various schemes have been proposed. These solutions can be divided into two general groups. The first group uses blocking, jamming and physical solutions to increase the security and privacy of RFID systems [45, 46, 47]. The other group uses cryptography to provide the security and privacy in RFID systems. Cryptographic solutions for RFID systems can themselves be divided into two main groups, light-weight and complex cryptographic solutions. Most RFID researchers believe that the industry needs simple and low cost RFID tags (below 5 cents per item) with limited number of logical gates. For this case, many approaches that are based on the light-weight cryptographic solutions and protocols have been suggested [30, 31, 32, 33, 34, 35, 36, 37, 38]. Light-weight cryptographic solutions have the advantage of keeping the computational demand and the price of RFID tags low. On the other hand, some researchers believe that it is possible to use more complex cryptographic protocols in future RFID tags. They suggest the use of public key solutions such as elliptic curve cryptography (ECC) [39, 40, 41, 42] and the advanced encryption standard (AES) [43]. A few approaches that cannot be categorized into these two main groups have also been proposed. For instance, Holcomb *et al.* have suggested the employment of the power-up static random access memory (SRAM) state as an identifying fingerprinting tool to solve the security problems of RFID tags [44].

Among the different solutions suggested for RFID security issues, one approach relies on the use of a *blocker tag*. A blocker tag is a cheap passive RFID device that can simulate many ordinary RFID tags simultaneously. When carried by a consumer, a blocker tag thus "blocks" RFID readers [45]. This approach has attracted much attention from both industrial and academic communities because of its simplicity and ease of implementation. This makes it an appropriate and inexpensive candidate for many future RFID applications.

In the blocker solution, when a blocker tag receives a query message from a reader, it can reply with some fake IDs to prevent the reader from successfully identifying the neighboring real tags by keeping the reader busy. This approach addresses the case where the tags are not removed from the sold items. When the customer goes to the checkout counter and pays for the merchandises, he/she receives a bag with a blocker tag inside it. When interrogated by a reader, this blocker tag generates and broadcasts fake serial numbers in response. The customer puts all the purchased items along with the blocker tag in a bag and leaves the store. On his/her way to home, the customer cannot be tracked successfully by any reader because of the blocker tag. Moreover, when the customer arrives home and brings the purchased items out of the bag, the originally attached RFID tags can be used again. For example, the customer can put a pack of food equipped with an RFID tag in an intelligent microwave and the microwave starts cooking the contained material based on the instructions kept by the tag [12]. A blocker tag is very similar to ordinary tags, and therefore, its price is acceptable (almost the same as ordinary tags) [19, 45]. This makes the blocker tag an ideal candidate and an economic solution for addressing the security concerns of many RFID applications.

The blocker tag approach, however, can itself introduce a different type of threat to the system. A malicious attacker can launch a blocking attack in a store or warehouse by placing a blocker tag inside that store. In this case, the blocker tag generates and broadcasts numerous serial numbers so as to mislead the legitimate reader and force the system to be engaged in time consuming and useless interrogation sequences. On the other hand, blocker tags are inexpensive, easy to implement, and they can solve the tracking and impersonation problems in passive RFID tags effectively. Briefly, the blocker tag solution could have played a significant role, probably as the best possible solution for many RFID applications, if the RFID users were not worried about the blocking attack. To detect the

blocker tag attack, an approach based on a pre-determined threshold can be used [45]. This approach, however, is computationally demanding (time-consuming) and could hinder the efficiency of the system. The motivation of our work is to design a lower layer algorithm that can detect the presence of blocker tags in passive RFID systems in a timely manner. The contributions of this chapter are as follows:

- We mathematically analyze the interrogation process of RFID systems which use the binary tree walking or ALOHA singulation mechanisms.
- To investigate the behavior of an RFID system in the presence of a blocker tag, we mathematically model the blocker attack problem using the information extracted from the queries performed by the reader.
- We propose a probabilistic blocker tag detection (P-BTD) algorithm to detect the presence of blocker tags in RFID systems.
- We determine the probability of false alarm for the P-BTD algorithm via simulations. The simulation results also show that our proposed P-BTD algorithm has better performance than the threshold-based detection algorithm in terms of having a shorter time (or needing fewer queries) to detect the presence of a blocker tag.

The rest of this chapter is organized as follows: In Section 2.2, we present the system model and problem formulation for RFID systems that operate based on the binary tree walking and ALOHA singulation mechanisms. In Section 2.3, we propose two P-BTD algorithms for detecting the presence of blocker tags in binary tree walking and ALOHA-based RFID systems. The performance comparison between our proposed P-BTD algorithms and the thresholding algorithms suggested in [45] is presented in Section 2.4. The chapter is summarized in Section 2.5.

2.2 System Model and Problem Formulation

In Section 2.2.1, we explain the system models for RFID systems that operate based on the binary tree walking and ALOHA tag singulation mechanisms. We also explain the blocking attack in binary tree walking and ALOHA tag singulation mechanisms. In the next step, we provide two probabilistic models for the binary tree walking and ALOHA singulation mechanisms in Section 2.3.

2.2.1 System Model

Because of the shared nature of the wireless channel in RFID systems, an RFID reader cannot communicate with more than a single tag at a time. If more than one tag responds to a query by the reader (for example, in Walmart's automated checkout gate), the reader detects a "collision" and will not be able to read the tag IDs transmitted by the tags accurately. Thus, the reader and the tags need to engage in a protocol that enables the reader to communicate with the nearby tags one at a time. Such a protocol is called a singulation protocol, and enables the reader to talk to each tag singly (one by one) [45]. Most of these singulation protocols can generally be classified into tree-based or ALOHA-based algorithms [48]. The tree-based methods, such as the binary tree walking and the query tree mechanisms, continuously divide a set of tags into two subsets until each subset has only one tag [45, 49, 51, 67, 87, 88]. Then, each tag ID can be obtained successfully by the reader. In the ALOHA-based mechanisms such as the dynamic frame-slotted ALOHA, the reader assigns a frame to all tags in the system. The frame consists of a limited number of time slots. Each tag chooses one time slot at random and transmits its information in that time slot [1, 53, 55, 57, 69, 73, 89, 90, 91, 92].

In Sections 2.2.1.1 and 2.2.1.2, we explain the system models for the binary tree walking and the ALOHA singulation mechanisms. The blocking attack is then discussed in Section

2.2.1.3.

2.2.1.1 Binary Tree Walking-based RFID Systems

The binary tree walking technique uses a tree to represent the existing tags in an RFID system. In this representation, each *leaf* of the tree has a unique ID. These IDs show the possible serial numbers which can be used by the tags in the RFID system. Each existing tag has its own ID which corresponds to a leaf in the binary tree. The number of the tags present in the system is less than or equal to the number of leaves in the binary tree. In other words, each tag in the system corresponds to a leaf in the binary tree but some of the leaves may not correspond to any tag in the system. The output of the binary tree walking algorithm yields a list of the IDs of the tags existing in the system. The tree has $(L+1)$ levels starting from level 0 and ending at level L, assuming that the ID of each tag is represented by a binary number of length L bits. The node at level 0 corresponds to the *root* node and does not have an address. The nodes located in levels 1 to $(L-1)$ are called the *interrogation nodes*. Any interrogation node at level l, where $l \in \{1, \ldots, L-1\}$, can be uniquely identified by a binary prefix $\boldsymbol{b}$ where

$$\boldsymbol{b} = b_1 b_2 \ldots b_l. \tag{2.1}$$

Fig. 2.1 shows the binary tree corresponding to a system with four-bit IDs (i.e., $L = 4$). In this figure, the interrogation nodes at level $l = 2$ are identified using the prefixes $\boldsymbol{b} = 00$, $\boldsymbol{b} = 01$, $\boldsymbol{b} = 10$ and $\boldsymbol{b} = 11$. In the binary tree walking algorithm, the reader initiates the interrogations at the root of the tree. At a given interrogation node at level l with prefix $\boldsymbol{b}$, the reader queries all the tags that correspond to the leaves of the subtree rooted at the node with prefix $\boldsymbol{b}$. All other tags should remain silent during this phase. The queried tags reply to the reader by announcing the $(l+1)$th bit in their serial numbers.

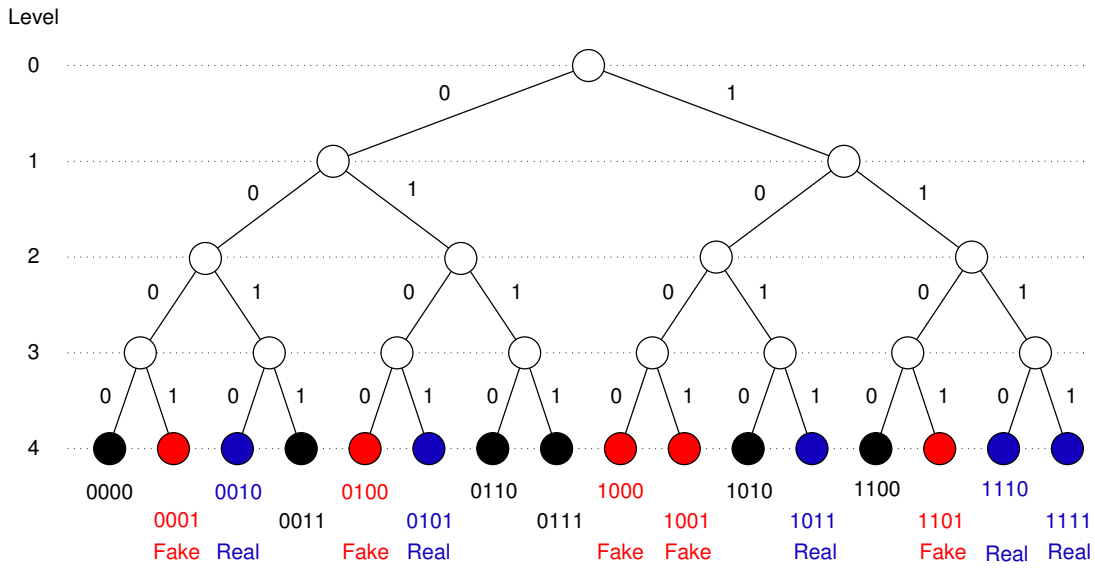

Figure 2.1: Binary tree walking mechanism for tag singulation.

The subtree rooted at the node with prefix $\boldsymbol{b}$ is composed of two subtrees, the left and right subtrees. In response to an interrogation, at a node with prefix $\boldsymbol{b}$, each tag broadcasts bit 0 if it lies in the left subtree and bit 1 if it lies in the right subtree. Considering this mechanism, two cases may arise. The first case is when both the left and right subtrees of the interrogation node have tags present. In this case, the reader observes a collision since the tags in the left and right subtrees transmit simultaneously. When a collision happens, the reader first moves to the child node with prefix $b_1b_2b_3 \dots b_l0$, i.e. the left hand side of the subtree. Starting from the child node with prefix $b_1b_2b_3 \dots b_l0$, the reader continues its interrogation until every leaf in that subtree is covered. Then, the reader moves to the child node with prefix $b_1b_2b_3 \dots b_l1$ on the right hand side of the node $\boldsymbol{b}$ to continue its interrogations. The second case arises when all the tags at node $\boldsymbol{b}$ reply with only a single bit b_{l+1} (0 or 1), which means that they all lie in the same subtree. In that case, the reader moves to the node with prefix $b_1b_2b_3 \dots b_lb_{l+1}$ and ignores the other subtree. When the algorithm reaches a leaf, the corresponding tag transmits its L-bit serial number. At the

end of this procedure, the output of the binary tree walking algorithm is a list of the serial numbers of all tags within the reader's range [45].

2.2.1.2 ALOHA-based RFID Systems

In recent years, different mechanisms for ALOHA-based tag singulation have been suggested [1, 53, 55, 57, 69, 73, 89, 90, 91, 92]. In the ALOHA-based tag singulation mechanisms, the reader interrogates all the tags and orders them to transmit their IDs in a predefined number of time slots, called a frame. At the beginning of a frame, the reader sends a query message containing the frame size to the tags. Each tag randomly chooses a time slot in the frame and transmits its ID in that time slot. If a specific time slot is chosen by only one tag, then the transmission of this tag is successful and the reader is able to read its information. If more than one tag chooses a certain time slot, a collision occurs and the reader is then not able to read the content of this time slot. A time slot is called empty if no tag transmits in that slot. In the ALOHA-based singulation mechanism, the reader interrogates the tags and reads the content of the time slots having one ID (single time slots). The reader continues this procedure repeatedly until it identifies all the existing tags in the system. In each interrogation, previously identified tags are instructed to remain silent, meaning that if a tag successfully transmits its ID in one interrogation, it will not send its ID in the next interrogations.

In the ALOHA model, the reader is responsible for determining the number of required time slots in each frame. If the number of time slots (in a frame) is too small compared to the number of tags, then many collisions happen and the reader will not be able to read the content of these collided time slots. On the other hand, if the number of time slots is much larger than the number of tags, then the reader observes many empty time slots. This means that the communication resources are not efficiently used and the reader is wasting part of its resources. The ideal case happens when the number of assigned time

slots is equal to the number of tags in the system [93]. However, the reader might not know the number of tags and it needs to approximate this value. Different techniques have been introduced so far to achieve this goal and to optimize the number of required time slots [1, 3, 53, 55, 73, 89, 90, 91, 93]. For example, Kodialam *et al.* have proposed that the reader estimates the number of RFID tags in the system using the number of empty time slots in each frame and then adjusts the length of the next frame based on this estimation [93].

2.2.1.3 Blocking Attack

Blocker tags have originally been suggested for the purpose of protecting the privacy of users and preventing unauthorized readers from successfully interrogating the nearby tags. It was first designed and introduced by Juels *et al.* based on the binary tree walking singulation technique, but it is mentioned in the paper that this idea can be extended for the ALOHA-based singulation techniques as well [45]. For RFID systems that use the binary tree walking mechanism, the malicious blocker chooses some leaves in the binary tree at random and replies to the reader if these leaves are interrogated as explained in Section 2.2.1.1. If the leaf chosen by the blocker represents a tag which really exists in the system, the blocker's response does not affect the final number of detected tags by the reader. However, if the chosen leaf was originally an empty leaf, the blocker's response causes the reader to assume that the leaf belongs to a real existing tag. We refer to this tag as a fake tag. For RFID systems which operate based on the ALOHA mechanism, the malicious blocker chooses some time slots at random and transmits some fake IDs in those time slots as explained in Section 2.2.1.2. If an attacked time slot represents a real (existing) tag, the reader observes collision in that time slot and cannot read the ID of the real tag. If the attacked time slot does not correspond to a real tag, it is considered as a single time slot and the reader considers its content (the fake ID) as the ID of a real

existing tag. In other words, we assume that the blocker attack does not affect collided time slots in a frame, but it can change an empty slot to a single slot or change a single slot to a collided slot.

It should be noted that the blocking attack is not limited to the RFID systems that use the blocker approach for privacy protection. Any passive RFID system that uses a singulation mechanism is also vulnerable to this attack. In other words, the blocker attack is a MAC-layer denial of service (DoS) threat that aims to prevent the reader from successfully interrogating the RFID tags in the system. A blocker tag can be placed in a store or warehouse by malicious attackers so as to sabotage or adversely affect the operation of the legitimate reader. We can assume two types of blocker tags. A *universal blocker tag* can simulate all possible RFID tag IDs while a *partial* or *selective* blocker tag can only simulate a selective range of IDs (e.g., the set of serial numbers assigned to a particular manufacturer) [45]. Such blocker tags can be used to disrupt business operations by shielding merchandises from the inventory control mechanism and delaying the whole procedure by forcing the reader to start a long sequence of useless interrogations. The universal blocker attack can be detected easily using some simple algorithms, however, it is not that easy to detect the presence of a selective blocker tag in an RFID system [45]. To the best of our knowledge, the main approach for detecting the presence of a blocker tag is based on the use of a pre-determined threshold [45]. In this approach, the reader stops its interrogation process after completing a predefined number of interrogations, or after detecting a specific number of tags. For instance, the reader can be programmed in such a way that it stops interrogation after detecting $(T + 1)$ tags, where T is the number of existing RFID tags in the system (if it is known) or it can be a certain predefined large number (if the actual number of existing tags is not known). The purpose of this chapter is to develop a more efficient way for detecting the presence of a malicious blocker tag in

a shorter period of time.

Many large companies, such as Wal-Mart and Procter and Gamble, currently use RFID tags to improve inventory accuracy, on-shelf availability and monitoring purposes. For instance, it has been estimated that only in the United States, Wal-Mart tags approximately 250 million men's jeans annually. The apparel items are tagged at the point of manufacturing, and they are read as they arrive at the loading docks, when they move from the warehouses to the sales floor, and on the shelves [94]. These tags are read frequently during working hours. Using this technique, the number of jeans and other items are checked over time to prevent the theft of items from the shelves. Moreover, the on-shelf monitoring system is notified if for instance, a specific size or model of an apparel is near to being sold out or is in high demand. This way, the store is able to keep the balance between consumer demand and the number of items on shelves. The following example shows the importance of developing an efficient blocker tag detection method. Assume that a branch of Wal-Mart orders 2500 jeans of different styles and different sizes. These jeans are tagged, stored in the warehouse, and moved to the sales floor as the previous items are being sold. An attacker can put a blocker tag in the warehouse to disrupt the inventory mechanism. If the universal attack is used in an RFID system which works based on the binary tree walking, the reader can easily detect this attack after finding a series of successive IDs (500 for instance), or after finding an unexpected ID in the system (some IDs may be reserved in the system [3, 45], or may belong to other goods or other manufacturers). This detection is even easier if the ALOHA technique is employed by the universal blocker. The attacker sends information in all the ongoing time slots, changing the empty slots to single slots and the single slots to collided ones. In this case, the reader can be programmed so that it announces the presence of an attacker if it does not observe any empty slot after checking a pre-defined number of frames. The bottom line for detecting the univer-

sal attack is counting the number of identified tags in the system and comparing it to a pre-defined threshold. However, the story is different for a selective attack. In the above example, the reader can detect the presence of a selective blocker only after identifying at least 2501 IDs in the singulation procedure (thresholding method). These 2501 IDs are not necessarily successive, therefore, it takes a long time for the reader to detect the 2501 IDs before terminating the singulation process. Moreover, some attackers may try to mislead the on-shelf inventory mechanism of a store. As an example, a malicious user can put a selective blocker among the apparels of the sales floor to convince the reader that there are enough jeans of a specific size on the shelf, to steal some items or to prevent the system from keeping the balance between the demand and the jeans required on the shelf. This type of attack is harder to detect, comparing to the universal blocking attack, and the store should be notified as soon as possible. Based on the above, large organizations and suppliers are vulnerable to blocking attacks, and they are in need of more efficient methods for detecting selective blocking attacks.

For different RFID applications, we may face two different scenarios. In the first scenario, accurate information about the number of existing RFID tags is not known. For example, RFID tags can be used to count the number of persons attending a conference or to have an estimate of the number of attendants in different sessions. In these types of applications, we do not know the exact number of RFID tags in the system. If a blocker tag is used by an attacker to corrupt this system, to the best of our knowledge, there is no efficient approach to make the reader capable of detecting the presence of the blocker tag. If we do not have any initial information about the RFID system and the attack model, it is not possible to design an efficient algorithm to detect the blocker attack in the system. In that case, we can only rely on some predefined thresholds and use them to instruct the reader to stop interrogation when the number of detected tags or the number

of interrogations exceeds the predefined thresholds.

In the second type of RFID applications, the reader has some initial information about the system. Assume a warehouse or a large store where, for example, the reader knows a priori how many bottles of wine (equipped with RFID tags) exist in the system (at the beginning). When a customer buys some bottles of wine, the number of purchased bottles is subtracted from the total number of bottles in the system. Therefore, the reader has always the updated information about the number of items equipped with RFID tags in the system. Another example is a library which uses RFID technology. Here, the exact number of books in the library is known to the RFID reader. If somebody borrows some books, then by moving through the RFID gate, the reader subtracts the number of detected books from the total available books in the library [21]. In these types of applications, the reader has initial information about the number of RFID items in the system. The question here is, how can we use a priori information to find an efficient way to reduce the vulnerability of RFID systems against the blocker attack? In this chapter, we answer this question and propose an efficient probabilistic approach to detect the existence of a blocker tag in the system.

2.2.2 Problem Formulation

The use of a pre-determined threshold to detect the presence of a malicious blocker tag in the system can be very time consuming. This is because the reader is obliged to continue searching for new serial numbers until a predefined number of interrogations (or a predefined number of detected tags) is accomplished. To provide a faster and more efficient blocker tag detection method, first we need to find a reliable analytical model for the blocking attack. In Section 2.2.2.1 and 2.2.2.2, we derive two probabilistic models for the binary tree walking and ALOHA tag singulation mechanisms.

2.2.2.1 Binary Tree Walking-based RFID Systems

We consider an RFID system in which there are N real (actual) tags. Let B denote the event that a blocker tag is present and let $\bar{B}$ denote the event that a blocker tag is not present. If a blocker tag is present, it can generate F different fake IDs when queried by the reader. Assume that the reader uses the binary tree walking algorithm for tag singulation. The total number of levels is L. We use $\boldsymbol{b} = b_1 b_2 \dots b_l$ to denote the prefix of the interrogation node. Based on the number of bits in $\boldsymbol{b}$, the corresponding level l can be determined accordingly. Let $N(\boldsymbol{b})$ and $E(\boldsymbol{b})$ denote the number of detected tags (both real and fake) and the number of empty positions in the left hand side of the interrogation node with prefix $\boldsymbol{b}$, respectively. The reader updates the values of $N(\boldsymbol{b})$ and $E(\boldsymbol{b})$ after each interrogation. For example, assume that the reader reaches the node with prefix $\boldsymbol{b} = 10$ in Fig. 2.1 but it has not interrogated the node $\boldsymbol{b} = 10$ yet. Thus, the reader would have observed $N(\boldsymbol{b}) = 4$ (for RFID tags with IDs 0001, 0010, 0100, and 0101) so far, and $E(\boldsymbol{b}) = 4$ (for empty positions 0000, 0011, 0110, and 0111) from its previous interrogations. When the reader queries a node with prefix $\boldsymbol{b}$, it observes one of the three possible responses which we denote by the set $r = \{0, 1, c\}$. The value of 0 or 1 corresponds to receiving bit 0 or 1, respectively. The value of c corresponds to a collision. For example, at the interrogation node with prefix $\boldsymbol{b} = 10$ in Fig. 2.1, the reader observes a collision because there exist three tags with 1000, 1001 and 1011 IDs under this interrogation node.

Given $N(\boldsymbol{b})$, $E(\boldsymbol{b})$, and the presence of a blocker tag (i.e., event B), the probability of observing $r = 0$ at the interrogation node with prefix $\boldsymbol{b}$ is the probability that there is at least one tag in the 0 branch of the subtree rooted at node with prefix $\boldsymbol{b}$ and there is no

tag in the 1 branch of this subtree. This probability can be written as

$$P_B(r=0 \mid N(\boldsymbol{b}), E(\boldsymbol{b})) = \sum_{i=1}^{2^{L-(l+1)}} \left(\binom{2^{L-(l+1)}}{i} \prod_{j=0}^{i-1} \left(\frac{[N+F-N(\boldsymbol{b})-j]^+}{2^L - N(\boldsymbol{b}) - E(\boldsymbol{b}) - j} \right) \times \prod_{m=i}^{2^{(L-l)}-1} \left(1 - \frac{[N+F-N(\boldsymbol{b})-i]^+}{2^L - N(\boldsymbol{b}) - E(\boldsymbol{b}) - m} \right) \right), \quad (2.2)$$

where $[x]^+ = \max\{x, 0\}$, $\prod_{j=0}^{i-1} \left(\frac{[N+F-N(\boldsymbol{b})-j]^+}{2^L - N(\boldsymbol{b}) - E(\boldsymbol{b}) - j} \right)$ is the probability that i leaves in the 0 branch of the interrogation node $\boldsymbol{b}$ are occupied, $\prod_{m=i}^{2^{(L-l)}-1} \left(1 - \frac{[N+F-N(\boldsymbol{b})-i]^+}{2^L - N(\boldsymbol{b}) - E(\boldsymbol{b}) - m} \right)$ is the probability that the remaining $\left(2 \times (2^{L-(l+1)}) - i\right)$ leaves in the 0 and 1 branches of the interrogation node are empty, and $\binom{2^{L-(l+1)}}{i}$ is the number of ways which we can choose i leaves out of the $(2^{L-(l+1)})$ leaves in the zero branch. We used the $[x]^+$ operator to guarantee that the number of occupied leaves cannot be more than the number of tags in the system.

The probability of observing $r = 1$ at the interrogation node with prefix $\boldsymbol{b}$ in the presence of a blocker is the probability that there is no tag in the left hand side (left branch) of the subtree rooted at $\boldsymbol{b}$ and there is at least one tag in the right hand side (right branch) of this subtree. This probability is equal to the probability of observing $r = 0$. Thus,

$$P_B(r=1 \mid N(\boldsymbol{b}), E(\boldsymbol{b})) = P_B(r=0 \mid N(\boldsymbol{b}), E(\boldsymbol{b})). \quad (2.3)$$

A collision may also occur at an interrogation node with prefix $\boldsymbol{b}$ if there are tags in both of the left and right hand sides of the subtree rooted at node $\boldsymbol{b}$. This probability can be

written as

$$\begin{aligned} P_B(r = c \mid N(\boldsymbol{b}), E(\boldsymbol{b})) &= 1 - P_B(r = 0 \mid N(\boldsymbol{b}), E(\boldsymbol{b})) - P_B(r = 1 \mid N(\boldsymbol{b}), E(\boldsymbol{b})) \\ &= 1 - 2P_B(r = 0 \mid N(\boldsymbol{b}), E(\boldsymbol{b})). \end{aligned} \tag{2.4}$$

Given there is a blocker tag, the probability of having $N(\boldsymbol{b})$ and $E(\boldsymbol{b})$ at the interrogation node with prefix $\boldsymbol{b}$ is

$$P_B(N(\boldsymbol{b}) = n, E(\boldsymbol{b}) = e) = \binom{n+e}{n} \prod_{i=0}^{n-1} \left(\frac{N+F-i}{2^L - i} \right) \prod_{j=0}^{e-1} \left(1 - \frac{N+F-n}{2^L - n - j} \right). \tag{2.5}$$

In (2.5), the first product term is the probability that $N(\boldsymbol{b})$ specified positions are occupied in the $(N(\boldsymbol{b}) + E(\boldsymbol{b}))$ possible positions. The second product term is the probability that the remaining $E(\boldsymbol{b})$ positions are empty.

Given there is a blocker tag, the probability that the reader receives a response r at node $\boldsymbol{b}$, and observes $N(\boldsymbol{b})$ detected tags and $E(\boldsymbol{b})$ empty positions is

$$P_B(r, N(\boldsymbol{b}), E(\boldsymbol{b})) = P_B(r \mid N(\boldsymbol{b}), E(\boldsymbol{b})) \times P_B(N(\boldsymbol{b}), E(\boldsymbol{b})). \tag{2.6}$$

Based on the probabilities in (2.2) and (2.5), the unconditional probability in (2.6) can be determined. Similarly, given that there is no blocker tag in the system, we can define the probabilities $P_{\bar{B}}(r \mid N(\boldsymbol{b}), E(\boldsymbol{b}))$, $P_{\bar{B}}(N(\boldsymbol{b}), E(\boldsymbol{b}))$, and $P_{\bar{B}}(r, N(\boldsymbol{b}), E(\boldsymbol{b}))$. We can obtain the corresponding values by substituting $F = 0$ (i.e., no fake tag in the system) into

(2.2)-(2.6). Thus, we have

$$P_{\bar{B}}(r=0 \mid N(\boldsymbol{b}), E(\boldsymbol{b})) = \sum_{i=1}^{2^{L-(l+1)}} \left(\binom{2^{L-(l+1)}}{i} \prod_{j=0}^{i-1} \left(\frac{[N-N(\boldsymbol{b})-j]^+}{2^L - N(\boldsymbol{b}) - E(\boldsymbol{b}) - j} \right) \times \prod_{m=i}^{2^{(L-l)}-1} \left(1 - \frac{[N-N(\boldsymbol{b})-i]^+}{2^L - N(\boldsymbol{b}) - E(\boldsymbol{b}) - m} \right) \right), \quad (2.7)$$

$$P_{\bar{B}}(r=1 \mid N(\boldsymbol{b}), E(\boldsymbol{b})) = P_{\bar{B}}(r=0 \mid N(\boldsymbol{b}), E(\boldsymbol{b})), \quad (2.8)$$

$$P_{\bar{B}}(N(\boldsymbol{b})=n, E(\boldsymbol{b})=e) = \binom{n+e}{n} \prod_{i=0}^{n-1} \left(\frac{N-i}{2^L - i} \right) \prod_{j=0}^{e-1} \left(1 - \frac{N-n}{2^L - n - j} \right), \quad (2.9)$$

and

$$P_{\bar{B}}(r, N(\boldsymbol{b}), E(\boldsymbol{b})) = P_{\bar{B}}(r \mid N(\boldsymbol{b}), E(\boldsymbol{b})) \times P_{\bar{B}}(N(\boldsymbol{b}), E(\boldsymbol{b})). \quad (2.10)$$

From (2.7) and (2.9), the unconditional probability in (2.10) can be determined.

At each interrogation node with prefix $\boldsymbol{b}$, we call the tuple $(r, N(\boldsymbol{b}), E(\boldsymbol{b}))$ observed by a reader as an event. For example, in Fig. 2.1, the event observed at node $\boldsymbol{b} = 10$ is $(r = c, N(\boldsymbol{b}) = 4, E(\boldsymbol{b}) = 4)$. Based on the observed event, the probabilities in (2.6) and (2.10) can be determined.

2.2.2.2 ALOHA-based RFID Systems

Same as RFID systems which use the binary tree walking as the singulation mechanism, RFID systems which use the ALOHA singulation mechanism are also vulnerable to blocking attacks. An attacker may disrupt these systems by sending fake IDs to the randomly selected time slots in each frame. The blocker causes the reader to detect fake tags by

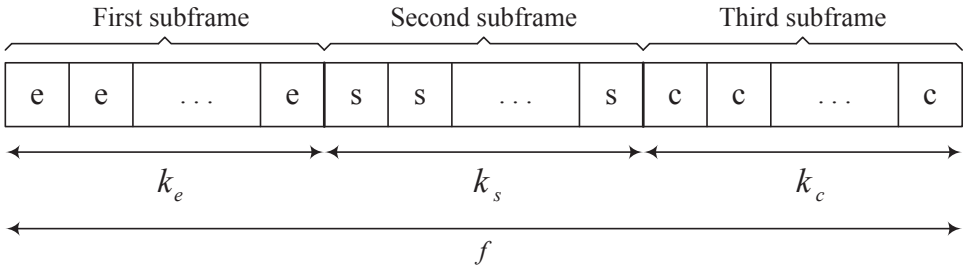

Figure 2.2: The empty, single and collided sections of a time frame in our analytical model.

sending fake IDs to the slots which would have remained empty in a normal system. Moreover, the blocking attack causes some of the singly occupied time slots to be observed as collided slots. Using this approach, the attacker can reduce the efficiency of the tag identification procedure drastically. Based on the above, we need to find an efficient way to make sure that there is no attacker in the system and prevent the reader from being involved in a loop of endless (or useless) interrogations. In order to do that, we analytically model the ALOHA tag singulation mechanism and find the probabilities that the reader observes a specific frame structure in presence and absence of a blocker tag. Then based on these probabilities, we decide whether the blocker exists or not.

For a query frame with length f in an ALOHA-based RFID system, let k_e denote the number of empty slots, k_s denote the number of slots with single transmission and k_c denote the number of collided slots. We denote the probability of observing k_e empty slots, k_s single slots, and k_c collided slots in the absence and presence of an attacker with $P_{\bar{B}}(k_e, k_s, k_c)$ and $P_B(k_e, k_s, k_c)$, respectively. Consider a frame structure which has three subframes as in Fig. 2.2. The first subframe has k_e empty slots, the second subframe has k_s single slots, and the last subframe consists of k_c collided slots. We first find the probability of observing such a frame and then use this probability to find $P_{\bar{B}}(k_e, k_s, k_c)$ and $P_B(k_e, k_s, k_c)$.

In the formulation, the frame length is denoted by f while N represents the number of

real tags in the system. First, the probability of observing k_e empty slots at the beginning of the frame is considered. This probability is denoted by $P_{\bar{B},1}(k_e)$ and is equal to

$$P_{\bar{B},1}(k_e) = \left(1 - \frac{k_e}{f}\right)^N . \tag{2.11}$$

In the next step, the probability of observing k_s single time slots in the second subframe conditioned to observing k_e empty slots in the previous step is obtained. This probability is denoted by $P_{\bar{B},2}(k_s \mid k_e)$

$$\begin{aligned} P_{\bar{B},2}(k_s \mid k_e) &= \binom{N}{k_s} \left(\frac{k_s}{k_s + k_c}\right)^{k_s} \left(1 - \frac{k_s}{k_s + k_c}\right)^{(N-k_s)} \\ &\times \left(\sum_{i=0}^{k_s} (-1)^i \binom{k_s}{i} \left(1 - \frac{i}{k_s}\right)^{k_s}\right), \end{aligned} \tag{2.12}$$

where the first three terms represent the probability that k_s tags out of N tags choose k_s slots in the second subframe and the remaining tags choose the last subframe. The last term in (2.12) is the probability that the k_s tags which have chosen the second subframe are assigned to the k_s slots *with no slot empty*. In other words, each of the k_s slots only accommodates one and only one of the k_s tags. This is a well-known problem in the classical urn model and the probability is provided in [95]. The last term in (2.12) can be simplified as

$$\sum_{i=0}^{k_s} (-1)^i \binom{k_s}{i} \left(1 - \frac{i}{k_s}\right)^{k_s} = \frac{k_s!}{k_s^{k_s}} . \tag{2.13}$$

Based on the above, $P_{\bar{B},2}(k_s \mid k_e)$ can be written as

$$\begin{aligned} P_{\bar{B},2}(k_s \mid k_e) &= \binom{N}{k_s} \left(\frac{k_s}{k_s+k_c}\right)^{k_s} \left(1-\frac{k_s}{k_s+k_c}\right)^{(N-k_s)} \frac{k_s!}{k_s^{k_s}} \\ &= \binom{N}{k_s} \left(\frac{k_c^{(N-k_s)}}{(k_s+k_c)^N}\right) k_s!. \end{aligned} \tag{2.14}$$

Now, we need to calculate the probability of observing k_c collisions in the last subframe conditional on observing k_e empty and k_s single time slots in the previous steps. This probability is denoted by $P_{\bar{B},3}(k_c \mid k_e, k_s)$. Since $(N-k_s)$ tags and k_c slots have left, this is the probability that $(N-k_s)$ tags are distributed in these slots in such a way that all slots have collisions. For $P_{\bar{B},3}(k_c \mid k_e, k_s)$, it is not that simple to calculate the probability of observing k_c collisions conditional on k_e and k_s *directly*. Let $g_{N-k_s}(k_c, 2)$ denote the number of possible ways of assigning $(N-k_s)$ tags to k_c slots while each slot contains at least 2 tags. Then, we have

$$P_{\bar{B},3}(k_c \mid k_s, k_e) = \frac{g_{N-k_s}(k_c, 2)}{k_c^{(N-k_s)}}, \tag{2.15}$$

in which $k_c^{(N-k_s)}$ is the total number of ways we can assign $(N-k_s)$ tags to the remaining k_c time slots. The work by Riordan [96] proved two closed form recursive expressions using the classical urn model for $g_n(m,s)$. We use one of the expressions which is

$$g_n(m,s) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} \frac{n!}{(s-1)!^k (n-sk+k)!} g_{n-sk+k}(m-k, s-1) \tag{2.16}$$

and $0 \leq g_n(m,s) < \infty$. Using (2.16), we can find the exact number of acceptable events in (2.15) by replacing n with $(N-k_s)$, m with k_c, and s with 2 for our problem. We can

simplify (2.16) by replacing s with 2 and write

$$g_n(m,2) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} \frac{n!}{(n-k)!} g_{n-k}(m-k,1) \tag{2.17}$$

in which

$$g_{n-k}(m-k,1) = p_0(n-k, m-k)\ (m-k)^{(n-k)}\ , \tag{2.18}$$

and $p_0(n-k, m-k)$ is the probability that we have $(n-k)$ tags and $(m-k)$ time slots and all the slots contain at least one tag. From [95], $p_0(n-k, m-k)$ can be expressed as

$$p_0(n-k, m-k) = \sum_{v=0}^{m-k} (-1)^v \binom{m-k}{v} \left(1 - \frac{v}{m-k}\right)^{(n-k)} . \tag{2.19}$$

Replacing (2.18) and (2.19) in (2.17), we have

$$g_n(m,2) = \sum_{k=0}^{m} \sum_{v=0}^{m-k} (-1)^{(k+v)} \binom{m}{k} \binom{m-k}{v} \frac{n!}{(n-k)!} (m-k-v)^{(n-k)}\ , \tag{2.20}$$

which gives us an explicit expression for $g_n(m,2)$. Using (2.11), (2.14), (2.15) and (2.20), $P_{\bar{B}}(k_e, k_s, k_c)$ can be written as

$$P_{\bar{B}}(k_e, k_s, k_c) = \left(\frac{f!}{k_e!\ k_s!\ k_c!}\right)\ P_{\bar{B},1}(k_e)\ P_{\bar{B},2}(k_s \mid k_e)\ P_{\bar{B},3}(k_c \mid k_s, k_e). \tag{2.21}$$

In (2.21), $\left(\frac{f!}{k_e!\ k_s!\ k_c!}\right)$ shows the number of ways the three mentioned subframes in Fig. 2.2 can be scrambled and mixed with each other and make a random structure of k_e empty slots, k_s single slots and k_c collided slots.

Now, we determine the probability of observing k_e empty, k_s single and k_c collided time slots in the presence of a blocker. To accomplish this task, we need to model the blocking

attack. We assume that an attacker exists in the RFID system and leaves each time slot intact (not blocked) with probability p while it blocks each time slot with probability $(1-p)$, and p can be varied between 0 and 1. Considering this model, the probability of observing k_e empty slots, k_s single slots and k_c collided slots in presence of a blocker is written as

$$P_B(k_e, k_s, k_c) = \left(\frac{f!}{k_e!k_s!k_c!}\right) P_{B,1}(k_e) \left[\sum_{i=0}^{k_s} P_{B,2}(k_s \mid k_e, i)\ P_{B,3}(k_c \mid k_e, k_s, i)\right]. \quad (2.22)$$

Here, $P_{B,1}(k_e)$, $P_{B,2}(k_s \mid k_e, i)$, and $P_{B,3}(k_c \mid k_e, k_s, i)$ are calculated using (2.23), (2.24) and (2.26), respectively. For $P_{B,1}(k_e)$, we have

$$P_{B,1}(k_e) = \left(1 - \frac{k_e}{f}\right)^N p^{k_e}, \quad (2.23)$$

in which $\left(1 - \frac{k_e}{f}\right)^N$ gives the probability that none of the N tags are assigned to the first k_e time slots and at the same time, the attacker does not block these k_e time slots in Fig. 2.2. For $P_{B,2}(k_s \mid k_e, i)$ we have

$$P_{B,2}(k_s \mid k_e, i) = \binom{N}{k_s - i} \left(\frac{k_s}{k_s + k_c}\right)^{(k_s-i)} \left(1 - \frac{k_s}{k_s + k_c}\right)^{N-(k_s-i)} p^{(k_s-i)} \times \frac{(k_s-i)!}{(k_s-i)^{(k_s-i)}} (1-p)^i \binom{k_s}{i} \left(\frac{k_s - i}{k_s}\right)^{(k_s-i)}, \quad (2.24)$$

in which $\binom{N}{k_s-i}$ is the number of ways we can choose $(k_s - i)$ tags out of the total N tags for the single subframe, $\left(\frac{k_s}{k_s+k_c}\right)^{(k_s-i)} \left(1 - \frac{k_s}{k_s+k_c}\right)^{N-(k_s-i)}$ gives the probability that $(k_s - i)$ tags are assigned to the single subframe and the remaining $(N - (k_s - i))$ tags are assigned to the collision subframe, $p^{(k_s-i)}$ is the probability that none of the $(k_s - i)$ time slots in the single subframe are blocked by the attacker, $\frac{(k_s-i)!}{(k_s-i)^{(k_s-i)}}$ is the probability that all the $(k_s - i)$ time slots are occupied by only one of the $(k_s - i)$ tags, $(1-p)^i$ gives the probability that

the i remaining time slots in the single subframe are all blocked by the attacker, $\binom{k_s}{i}$ is the number of ways we can choose i attacked slots out of k_s time slots in the single subframe, and $\left(\frac{k_s-i}{k_s}\right)^{(k_s-i)}$ gives the probability that (k_s-i) tags are assigned to the (k_s-i) slots out of the whole k_s time slots in the single subframe. Based on the above, (2.24) can be simplified as

$$P_{B,2}(k_s \mid k_e, i) = \binom{N}{k_s - i}\binom{k_s}{i}\left(\frac{k_c^{(N-k_s+i)}}{(k_s+k_c)^N}\right)(k_s-i)!p^{(k_s-i)}(1-p)^i. \tag{2.25}$$

For the $P_{B,3}(k_c \mid k_e, k_s, i)$ part, we have

$$P_{B,3}(k_c \mid k_e, k_s, i) = \begin{cases} 0\ , & k_c > N-k_s+i \\ \frac{k_c!}{k_c^{k_c}}(1-p)^{k_c}\ , & k_c = N-k_s+i \\ \sum_{j=0}^{k_c-1} \frac{g_{N-k_s+i-j}(k_c-j,2)}{(k_c-j)^{(N-k_s+i-j)}}\binom{k_c}{j}\binom{N-k_s+i}{j}\left(\frac{j!}{j^j}\right)\left(\frac{j}{k_c}\right)^j & \\ \times\left(\frac{k_c-j}{k_c}\right)^{(N-k_s+i-j)}(1-p)^j\ , & \text{otherwise} \end{cases} \tag{2.26}$$

where $g_{N-k_s+i-j}(k_c-j,2)$ is the number of ways we can assign $(N-k_s+i-j)$ tags to (k_c-j) time slots and each slot contains at least two tags, $\binom{k_c}{j}$ is the number of ways that we can choose j slots out of k_c for being blocked by the attacker, $\binom{N-k_s+i}{j}$ is the number of ways we can choose j tags out of $(N-k_s+i)$ to occupy these attacked time slots, $\left(\frac{j!}{j^j}\right)$ is the probability that all the j attacked time slots are occupied using exactly j tags, $\left(\frac{j}{k_c}\right)^j\left(\frac{k_c-j}{k_c}\right)^{(N-k_s+i-j)}$ is the probability that j tags are assigned to j number of the k_c time slots and the remaining $(N-k_s+i-j)$ tags are assigned to the remaining (k_c-j) time slots, and finally $(1-p)^j$ is the probability that these j time slots are blocked by the attacker.

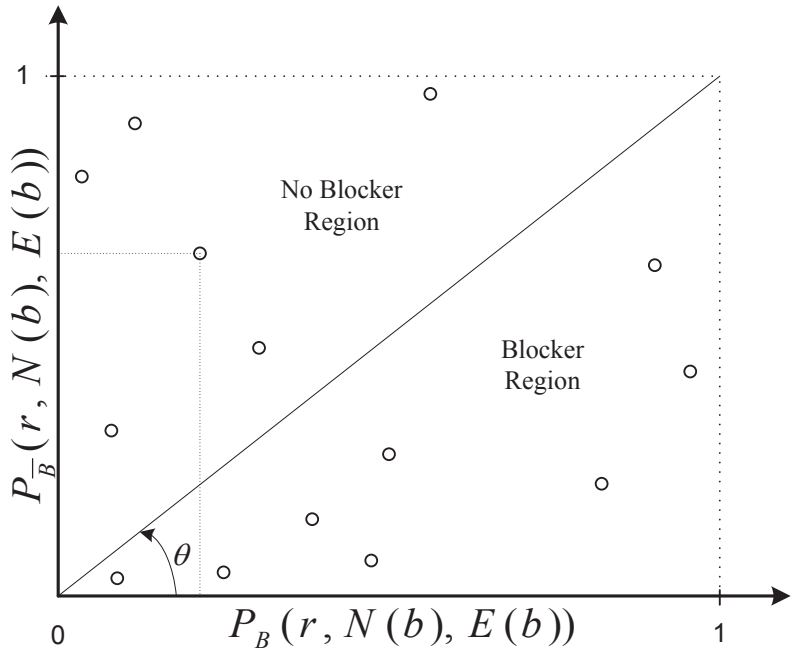

Figure 2.3: Two-dimensional representation of the events and decision making criterion for tree-based RFID systems.

2.3 Probabilistic Blocker Tag Detection (P-BTD) Algorithm

In this section, we use the analytical models developed in Sections 2.2.2.1 and 2.2.2.2 and propose two probabilistic blocker tag detection algorithms for RFID systems that operate based on the binary tree walking and ALOHA tag singulation mechanisms.

2.3.1 Binary Tree Walking-based RFID Systems

After finding the $P_B(r, N(\boldsymbol{b}), E(\boldsymbol{b}))$ and $P_{\bar{B}}(r, N(\boldsymbol{b}), E(\boldsymbol{b}))$ probabilities in Section 2.2.2.1, we can use them to decide whether there exists a blocker in the system or not. In order to do that, consider the two-dimensional space in Fig. 2.3, where the x-axis and y-axis denote $P_B(r, N(\boldsymbol{b}), E(\boldsymbol{b}))$ and $P_{\bar{B}}(r, N(\boldsymbol{b}), E(\boldsymbol{b}))$, respectively. Each point (or circle) in this space

corresponds to a feasible event and its location corresponds to the conditional probabilities in (2.6) and (2.10). Two regions can be defined on the two-dimensional space. The first region is the *blocker region* and the second one is the *no blocker region*. A blocker tag (or attack) is announced if the observed event resides in the blocker region of the two-dimensional space. The blocker and no blocker regions are separated using a line with the angle $\theta = 45$ degree as depicted in Fig. 2.3. Thus, a reader will declare that a blocker tag exists in the system if

$$P_B(r, N(\boldsymbol{b}), E(\boldsymbol{b})) > P_{\bar{B}}(r, N(\boldsymbol{b}), E(\boldsymbol{b})). \tag{2.27}$$

Algorithm 2.1 denotes the P-BTD procedure for determining the existence of a blocker tag in RFID systems which operate based on the binary tree walking mechanism. The input parameters of the P-BTD algorithm are the total number of levels L, the threshold T, the number of real tags N, the number of fake tags F, and the step size h. The step size h is a positive integer which tells the reader after how many interrogations it should decide about the existence of the blocker tag. The algorithm begins interrogation at the root of the tree. In line 2, N_l and E_l are auxiliary variables used to keep track of the number of tags and empty slots detected and they are used to update $N(\boldsymbol{b})$ and $E(\boldsymbol{b})$. In line 3, the reader sends a query to all the tags in the system and waits for their responses. Based on the responses from the tags, the reader will set the response r to 0, 1 or c. After that, the interrogation node $\boldsymbol{b}$ (i.e., the subtree) for the next interrogation is set accordingly. After every h interrogations, the reader decides about the existence of a blocker (line 9). Here, MOD shows the reminder of dividing *counter* by h. In lines 10 and 11, the required probabilities are determined from (2.6) and (2.10), based on the observed event. If equation (2.27) is satisfied, the reader announces the existence of a blocker tag and terminates the interrogation procedure (lines 12-13). Otherwise, the algorithm continues as follows.

Algorithm 2.1 P-BTD algorithm for binary tree walking-based RFID systems

1: Input L, T, h, N, F
2: $N_l := 0,\ E_l := 0$
3: Interrogate all tags and set r
4: Move to the next interrogation node and set $\boldsymbol{b}$
5: Set $N(\boldsymbol{b}) := N_l,\ E(\boldsymbol{b}) := E_l$
6: $counter := 0$
7: **while** $N(\boldsymbol{b}) + E(\boldsymbol{b}) \leq 2^L$
8: Interrogate at node with prefix $\boldsymbol{b}$ and set r
9: **if** $MOD(counter, h) = 0$
10: Compute $P_B(r, N(\boldsymbol{b}), E(\boldsymbol{b}))$ from Eq. (2.6)
11: Compute $P_{\bar{B}}(r, N(\boldsymbol{b}), E(\boldsymbol{b}))$ from Eq. (2.10)
12: **if** $P_B(r, N(\boldsymbol{b}), E(\boldsymbol{b})) > P_{\bar{B}}(r, N(\boldsymbol{b}), E(\boldsymbol{b}))$
13: Return: *Blocker exists*
14: **end if**
15: **end if**
16: **if** $r \in \{0, 1\}$ and $l = L - 1$
17: $N_l := N_l + 1$
18: **else if** $r = c$ and $l = L - 1$
19: $N_l := N_l + 2$
20: **end if**
21: **if** $N_l \geqslant T$
22: Return: *Blocker exists*
23: **end if**
24: $E_l := \text{decimal}(\boldsymbol{b}) \times 2^{L-l} - N_l$
25: Move to the next interrogation node and set $\boldsymbol{b}$
26: $counter := counter + 1$
27: Set $N(\boldsymbol{b}) := N_l,\ E(\boldsymbol{b}) := E_l$
28: **end while**

In lines 16-20, the algorithm updates the total number of tags detected in the system. The algorithm checks if the interrogation node is at level $(L - 1)$ or not. Observing a response r equals to either 0 or 1 at level $(L - 1)$ means that there exists only one tag in the two positions under that interrogation node. Therefore, N_l is incremented by 1. On the other hand, observing a collision at level $(L - 1)$ means that both positions under the interrogation node are occupied. Therefore, N_l is incremented by 2. In line 21, the algorithm also compares N_l and T. If the estimation of the number of real RFID tags N

is accurate, then T is set to $(N+1)$. Otherwise, we set T to a large value. In both cases, T is greater than N in Algorithm 2.1. In line 21, if $N_l \geqslant T$ (i.e., the reader has detected more tags than the threshold T), then the reader declares that a blocker exists and stops interrogation. If none of the two conditions in lines 12 and 21 holds, then the reader does not have enough evidence to conclude that there exists a blocker in the system. In line 24, the algorithm calculates E_l based on the values of N_l and $\boldsymbol{b}$, where the function decimal($\boldsymbol{b}$) converts the binary prefix $\boldsymbol{b}$ to a decimal value. After that, the algorithm moves to the next interrogation node and goes back to line 7. The algorithm stops by either announcing that a blocker exists or by checking all subsequent interrogation nodes in the binary tree.

If an attacker wants to disrupt an RFID system severely, it needs to block a large number of tags in the system. In other words, the larger the number of tags it blocks, the more severe is the attack. For example, we may expect that a harmful attacker needs to attack *at least* 20% of the total possible IDs to interrupt the interrogation procedure of the legitimate reader severely. In a 16-bit system, this means that the attacker needs to block at least 13000 IDs to make a severe problem for the legitimate reader.

2.3.2 ALOHA-based RFID Systems

Our approach for designing the P-BTD algorithm for ALOHA-based RFID systems is exactly the same as that of Section 2.3.1. First, we calculate $P_B(k_e, k_s, k_c)$ and $P_{\bar{B}}(k_e, k_s, k_c)$ using Eq. (2.21) and (2.22). Then, we divide the two dimensional space of the events observed by the reader into two regions as shown in Fig. 2.4, the blocker region and the no blocker region. Now we need an algorithm which helps the reader to detect a blocker in the system using the information obtained from the previous queries. This procedure is explained in Algorithm 2.2. The reader needs the initial values of N, p, T, and h. Here, T is a predefined threshold which can be adjusted by the user to determine the maximum

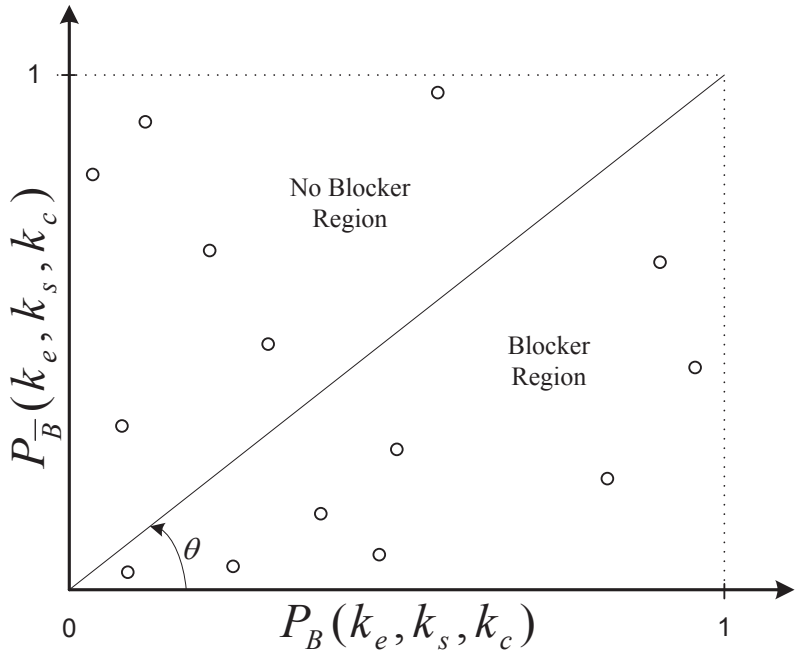

Figure 2.4: Two-dimensional representation of the events and decision making criterion for ALOHA-based RFID systems.

number of acceptable interrogations, h is the step size and N and p were defined previously. Using these values, the reader starts interrogating the tags and updates the values of N after each interrogation. The reader computes the values of $P_{\bar{B}}(k_e, k_s, k_c)$ and $P_B(k_e, k_s, k_c)$ after each h interrogations and compares them. If the value of $P_B(k_e, k_s, k_c)$ is greater than $P_{\bar{B}}(k_e, k_s, k_c)$, then it announces that there exists an attacker in the system and terminates the interrogation procedure, otherwise, it updates the values of $Query$, N, k_e, k_s, k_c and $Flag$, and continues its work. At each interrogation, the reader checks three conditions and if any of them does not hold, it terminates the interrogation immediately. The first condition, $(N > 0)$, guarantees that the number of detected tags is not bigger than the total number of RFID tags in the system. The second condition, $(Query < T)$, guarantees that the number of performed interrogations is less than a predefined threshold. Finally, $(Flag = 0)$ guarantees that no blocker has been detected in the system so far. In line 15, MOD is used to show the reminder of dividing $Query$ by h.

Algorithm 2.2 P-BTD algorithm for ALOHA-based RFID systems

Input N, p, T, h
$Flag := 0$
$Query := 0$
$k_e := 0$, $k_s := 0$, $k_c := 0$
while $(N > 0)$ **and** $(Flag = 0)$
  $f := N$
  Interrogate all tags
  $Query := Query + 1$
  if $Query > T$
    Return: *Blocker exists*
    $Flag := 1$
  end if
  update $k_e,\ k_s,\ k_c$
  $N := N - k_s$
  if $MOD(Query, h) = 0$
    Compute $P_{\bar{B}}(k_e, k_s, k_c)$ from Eq. (2.21)
    Compute $P_B(k_e, k_s, k_c)$ from Eq. (2.22)
    if $P_B(k_e, k_s, k_c) > P_{\bar{B}}(k_e, k_s, k_c)$
      Return: *Blocker exists*
      $Flag := 1$
    end if
  end if
end while

2.4 Performance Evaluation

This section presents the results of the simulation experiments we carried to evaluate the performance of our proposed P-BTD algorithms. We also present the performance comparisons between the proposed P-BTD algorithms and the threshold-based detection method [45]. All simulations are performed in the MAPLE environment.

2.4.1 Binary Tree Walking-based RFID Systems

In this part, we investigate the performance of the P-BTD algorithm when the interrogation process is based on the binary tree walking singulation. First, we consider the probability of

detection error. There are two types of detection errors for the proposed P-BTD algorithm. The first one is the error of missing the presence of a blocker. This happens when there exists a blocker in the system but the algorithm does not detect it. This probability is zero due to the fact that even if the probabilistic approach (i.e., line 12 in Algorithm 2.1) cannot detect a blocker, the threshold in line 21 of Algorithm 2.1 would detect it. Therefore, if a blocker exists, the algorithm detects its presence with probability one. The second error is *false alarm*. This happens when the algorithm declares that there is a blocker in the system but that is not the case. We find the probability of false alarm via simulations.

We consider an RFID system with 16-bit tag IDs (i.e, $L = 16$). In Algorithm 2.1, we set the input parameters as follows: $L = 16$, $T = N + 1$, $h = 1,000$ and $F = 1,000$, where N is the number of existing real tags, h is the step size and F is the number of fake tags generated by the blocker. N is varied from 1,000 to 5,000 with steps of 1,000. Fig. 2.5 shows the probability of false alarm. Simulation results show that the probability of false alarm decreases as the number of existing real tags N increases. When $N = 5,000$, the probability of false alarm is almost zero. This is because as N gets larger than F, the system becomes less sensitive to a blocker tag.

Next, we investigate the effects of changing the parameter F on the behavior of the system. In this experiment, $L = 16$, $N = 5,000$, and $h = 1,000$. We vary the number of fake tags F between 1,000 and 5,000. For different values of F, Fig. 2.6 shows the probability of observing a collision at the interrogation node with prefix $\boldsymbol{b} = 000000111110100$, given $N(\boldsymbol{b})$ and $E(\boldsymbol{b})$. Here, $N(\boldsymbol{b})$ shows the number of tags detected by the reader up to node $\boldsymbol{b}$ in the binary tree. The number of empty leaves detected by the reader up to node $\boldsymbol{b} = 000000111110100$ is given by $E(\boldsymbol{b})$. Fig. 2.6 shows that when the number of fake tags F increases, the distance between the two peaks related to the system with and without an attacker also increases. As this distance increases, the level of uncertainty in the de-

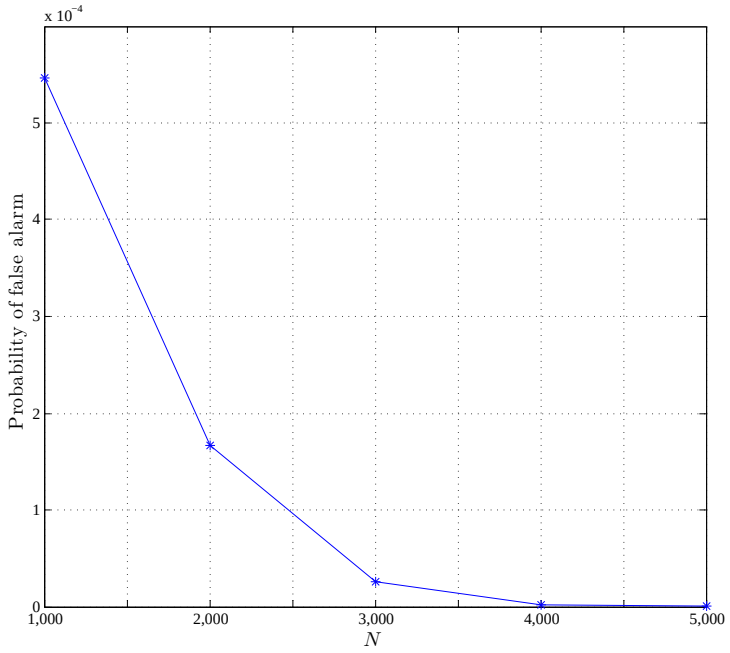

Figure 2.5: Probability of false alarm by P-BTD algorithm in a 16-bit RFID system.

cision decreases. This makes it easier for the algorithm to decide about the existence of an attacker. In other words, if the attacker reduces the number of fake tags it introduces, the two peaks in Fig. 2.6 merge and this increases the level of uncertainty. On the other hand, the attacker needs to block a large number of IDs in order to prevent the reader from identifying the real tags efficiently [45]. This makes it easier for the algorithm to detect the presence of the attacker. Although Fig. 2.6 is plotted for the collision event (i.e., $r = c$), we obtain similar results for the cases of receiving 0 ($r = 0$) or 1 ($r = 1$) by the reader.

We now compare the performance of the P-BTD algorithm with the threshold-based detection method [45] for a 16-bit RFID system. First, we set N = 5,000, h =1,000 and vary the number of fake tags F from 1,000 to 5,000. This procedure is repeated 1,000 times. Each time Algorithm 2.1 announces that a blocker exists, we save the binary ID number of the last detected tag before the algorithm makes this decision. At the end of the simulation, the saved IDs are averaged to form the average of the last detected ID. The

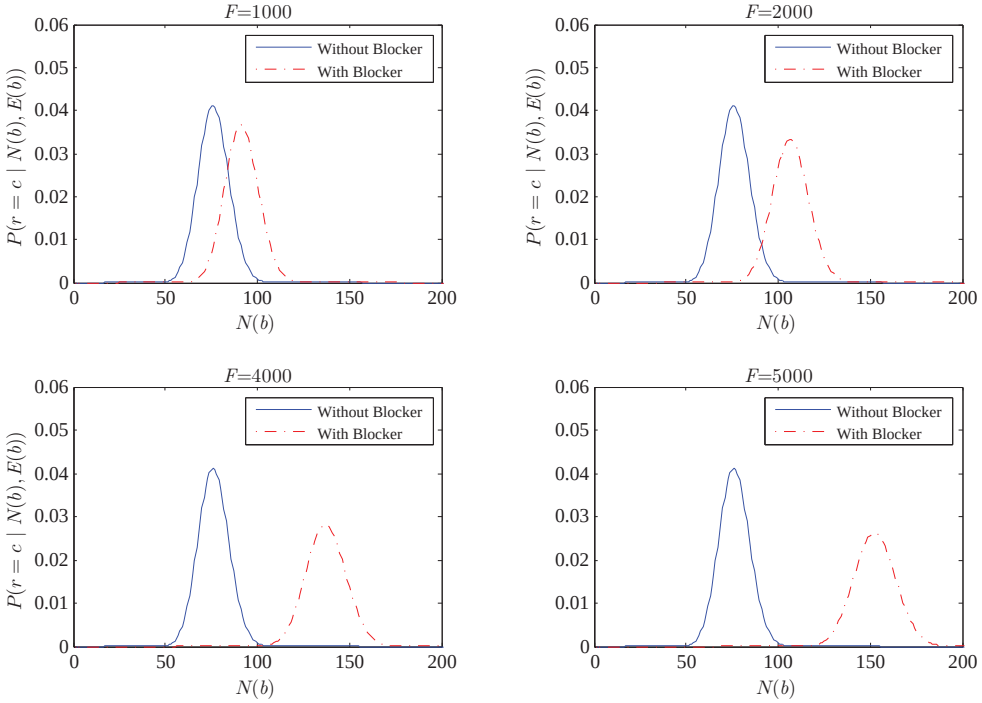

Figure 2.6: The effect of changing the number of fake tags on the probability of observing collision in an RFID system with $L = 16$, $N = 5,000$, $\boldsymbol{b} = 000000111110100$, and $h = 1,000$.

performance metric of the system is taken as the *average of the last detected ID numbers* before the algorithm declares a blocker exists. The reason this average is considered as an indicator of how fast the algorithm can detect the presence of a blocker tag is as follows: A small value for the last detected ID implies that the algorithm is able to detect a blocker with a few number of interrogations. In other words, the reader needs to perform more interrogations to find a tag whose ID value is large. Each interrogation takes a specific amount of time to accomplish, thus if fewer tags were interrogated, then less time is spent by the reader to make its decision. For ease of understanding, we convert the ID numbers from binary to a decimal format.

Fig. 2.7 shows the results of the last interrogated ID numbers averaged over 1,000 iterations (N = 5,000) for the threshold-based detection algorithm [45] and our proposed

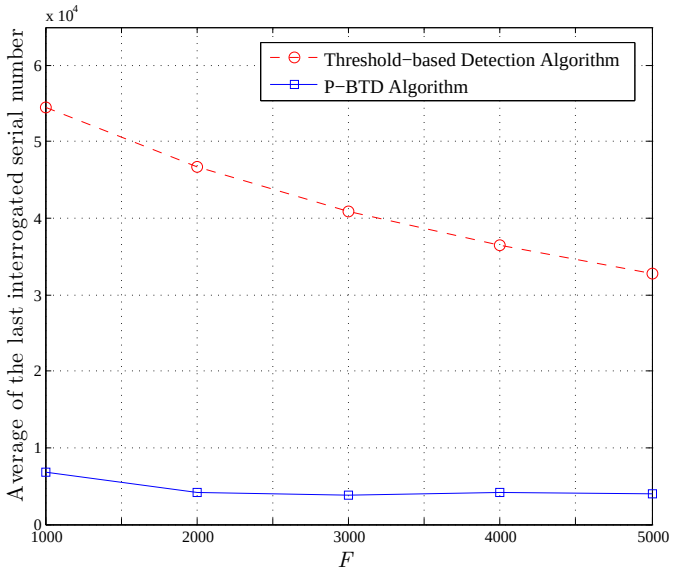

Figure 2.7: Average of the last detected ID before detecting the presence of a blocker versus number of fake tags F. ($L = 16$, $N = 5,000$ and $h = 1,000$)

P-BTD algorithm. Simulation results show that our proposed algorithm can detect the presence of a blocker at least 6 times faster than the threshold-based detection protocol [45] for different values of F. From Fig. 2.7, it can also be concluded that the detection speed of our proposed algorithm does not depend on F (for values of F greater than 2,000). Next, we present the simulation results when the number of existing tags N is varied. Again, the performance metric is the average of the last detected ID numbers. The number of fake tags F is set to 5,000. N is varied from 1,000 to 5,000 with steps of 1,000. The simulation results in Fig. 2.8 show that our proposed P-BTD algorithm is able to detect the blocker in the system faster (2.5 to 6.5 times) than the threshold-based method and with fewer interrogations. As can be inferred from Fig. 2.8, the threshold-based detection algorithm is sensitive to the number of real tags and its detection capability degrades as N increases. Our P-BTD algorithm outperforms the threshold-based algorithm in terms of detection time. Moreover, the performance of our proposed P-BTD algorithm does not depend on the the number of existing tags in the system. This can add to the value of

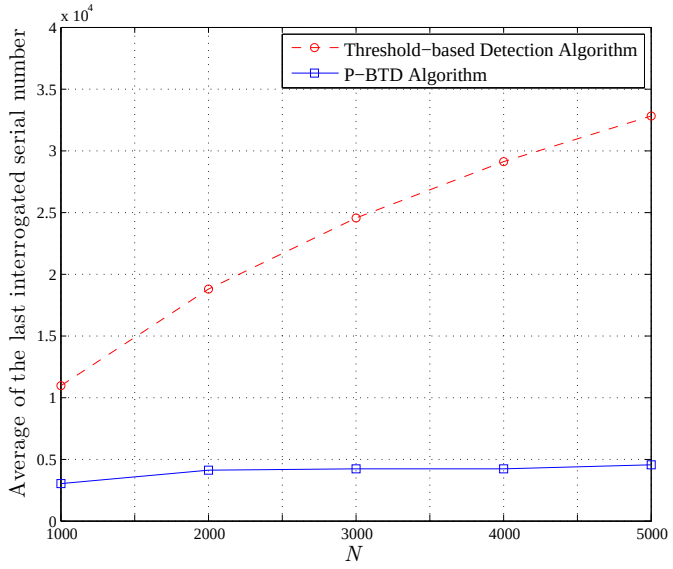

Figure 2.8: Average of the last detected ID before detecting the presence of a blocker versus number of real tags N. ($L = 16$, $F = 5,000$ and $h = 1,000$)

our proposed algorithm because in practical cases, the algorithm should be able to work efficiently irrespective of the value of N.

So far, we have assumed that we know the accurate values of N and F in the binary tree walking-based P-BTD algorithm. Now, we assume that the reader does not know the accurate values of these parameters and find the sensitivity of the P-BTD method to these values. In order to do that, we consider the cases where the P-BTD algorithm uses inaccurate values of N and F. Fig. 2.9 shows the average of the last detected IDs when the P-BTD algorithm uses inaccurate values of F with $\pm 5\%$ error in the binary tree walking system. Here, we assume $N = 5,000$ and $h = 1,000$. As can be inferred from Fig. 2.9, the P-BTD algorithm is capable of detecting a blocker tag faster (1.6 to 2.5 times) than the threshold-based method even when the reader uses inaccurate values of F (with $\pm 5\%$ error).

Fig. 2.10 shows the average of the last detected IDs when the P-BTD algorithm uses an inaccurate value of N (with $\pm 5\%$ error) in the binary tree walking system. Even in this

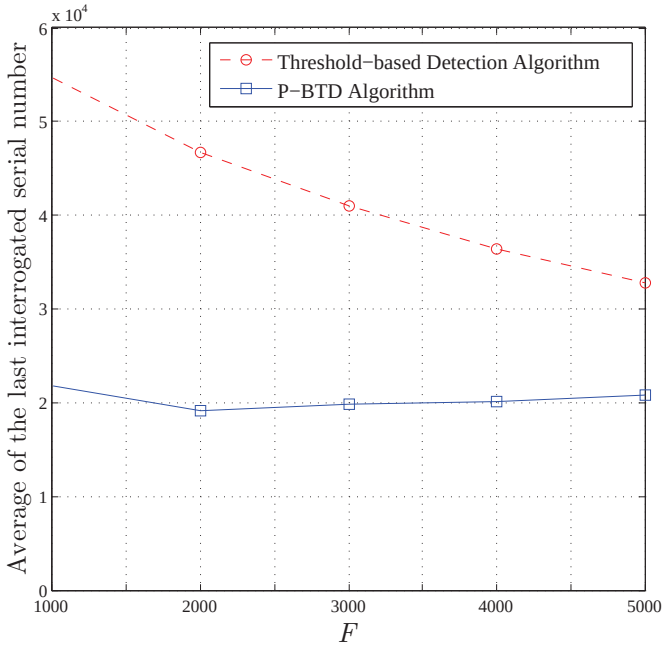

Figure 2.9: Average of the last interrogated serial number versus inaccurate values of F ($\pm 5\%$ error) in the P-BTD and threshold-based algorithms for binary tree walking RFID systems. ($L = 16$, $N = 5,000$ and $h = 1,000$)

case, the P-BTD algorithm is capable of detecting a blocker tag faster (1.1 to 1.8 times) than the threshold-based method.

2.4.2 ALOHA-based RFID Systems

For the ALOHA-based systems, we first investigate the performance of the P-BTD method in terms of the probability of false alarm. Fig. 2.11 shows the probability of false alarm for different values of N. We assume that $(1-p)$ is the probability of blocking any time slot by the blocker. We assume $p = 1$ for the case that a blocker does not exist and $p = 0.7$ for the case that a blocker exists. We vary N from 100 to 500 and repeat the experiment 10,000 times for each value of N. Then, we count the number of times the P-BTD algorithm announces the existence of a blocker in the system, when such a blocker does not exist. As we can conclude from the figure, the probability of false alarm increases as N increases.

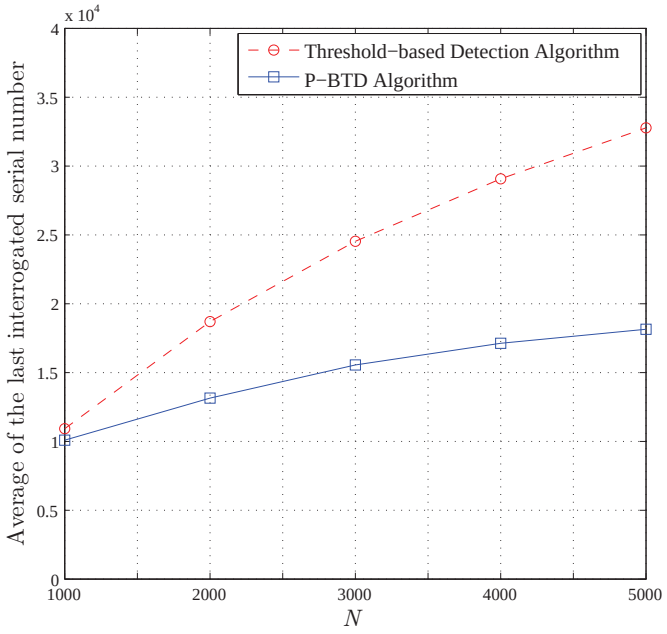

Figure 2.10: Average of the last interrogated serial number versus inaccurate values of N ($\pm 5\%$ error) in the P-BTD and threshold-based algorithms for binary tree walking RFID systems. ($L = 16$, $F = 5,000$ and $h = 1,000$)

The probability of false alarm is zero for the threshold-based detection algorithm. The average number of queries required to detect the presence of a blocker versus p is shown in Fig. 2.12. From this figure, we understand that the threshold-based algorithm is more dependent on the value of p than the P-BTD algorithm in terms of the average number of queries. Moreover, the P-BTD algorithm is capable of detecting the blocker faster (1.5 to 2.5 times) than the threshold-based method. This difference becomes more obvious in the region where p changes between 0.9 and 0.99. By increasing the value of p, the system behaves more similarly to a normal system (without a blocker). Therefore, more queries are needed to detect the blocker in the system. The average number of queries required for detecting the blocker versus N is shown in Fig. 2.13. As can be inferred from this figure, the P-BTD algorithm is able to detect the existence of an attacker using few queries (less than 3 queries) for different values of N while the threshold-based algorithm, on average,

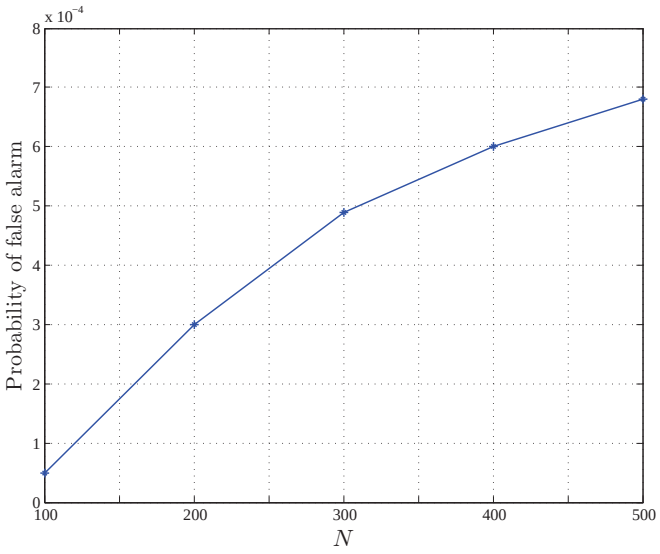

Figure 2.11: The probability of false alarm by P-BTD algorithm in an ALOHA-based RFID system.

detects the attacker close to the 6th query.

So far, we have assumed that the values of N and p are known in the ALOHA-based P-BTD algorithm. Now, we assume that the reader does not know the accurate values of these parameters and find the sensitivity of the P-BTD method to these values. In order to do that, we consider the cases where the P-BTD algorithm uses inaccurate values of N and p. Fig. 2.14 shows the average number of the required queries for inaccurate values of p in an ALOHA-based RFID system with $N = 500$. To model the error, we run the algorithm twice, using two inaccurate values of p. The error of p in the first run is -0.05 and the error in the second run is +0.05. Fig. 2.14 shows the average of the results for both cases. As can be observed, the P-BTD algorithm is capable of detecting the blocker tag faster (1.1 to 1.8 times) than the threshold-based method, even when the reader does not choose the right value for p. Fig. 2.15 shows the average number of required queries when the reader chooses an inaccurate value for N and p is equal to 0.7. Here, we assume the reader has $\pm 5\%$ error in choosing the right value of N. This situation can be ignored

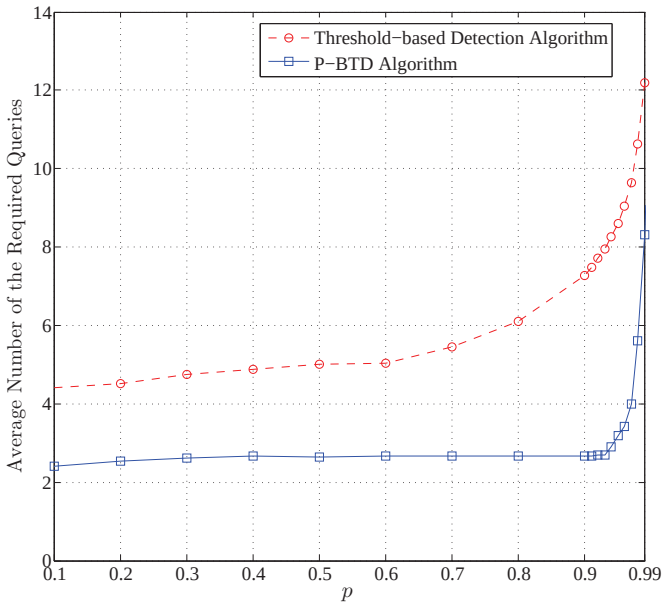

Figure 2.12: Average number of the required queries for different values of p in the P-BTD and threshold-based algorithms. ($N = 500$, $h = 1$ and $T = 21$)

in our P-BTD method because this algorithm is designed for applications where the initial value of N is known a priori and the changes of N over time can be tracked by the reader. As can be inferred from Fig. 2.15, the threshold-based algorithm is not capable of detecting the presence of the blocker if it does not have the correct value of N. Here, the algorithm terminates only after it reaches a predefined number of queries (21 in the simulations) by announcing that there exists a blocker in the system and stopping the interrogation procedure. On the other hand, the P-BTD algorithm is still capable of detecting the blocker tag but the number of required queries increases with N.

2.5 Summary

In this chapter, we studied the use of a blocker tag as a malicious tool to attack RFID systems. We modeled the blocker attack analytically for RFID systems whose interrogation

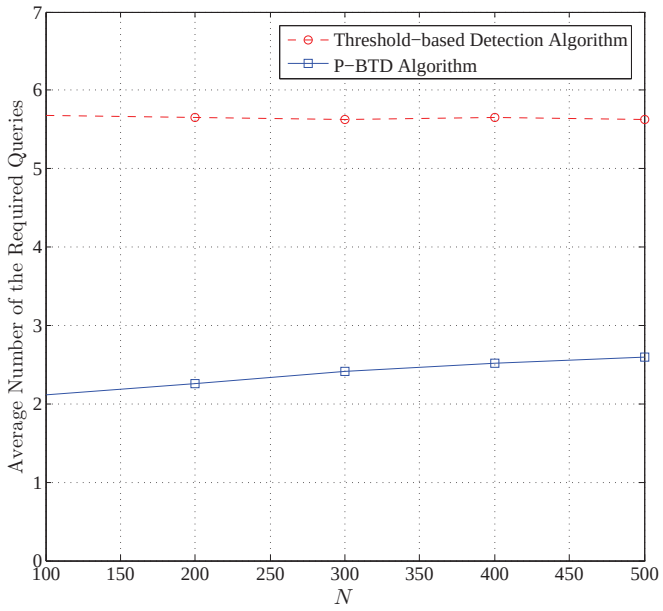

Figure 2.13: Average number of the required queries for different values of N in the P-BTD and threshold-based algorithms. ($p = 0.7$, $h = 1$ and $T = 21$)

processes are based on the binary tree walking or the ALOHA singulation mechanisms. Using these analytical models, we proposed two probabilistic blocker tag detection (P-BTD) algorithms. These algorithms use probabilistic approaches for detecting the presence of a blocker tag in RFID systems. The first algorithm is designed for RFID systems based on the binary tree walking concept and the second one is for ALOHA-based RFID systems. In the binary tree walking P-BTD algorithm, the RFID reader uses the information extracted from the previous interrogations along with the observation at the current interrogation node to make a decision about the existence of a blocker. In the ALOHA-based P-BTD algorithm, the reader uses the information obtained from each interrogation and updates the number of empty, single and collided time slots in the frame. Using this information, the reader calculates the probability of observing each frame structure in the presence and absence of a blocker and makes its decision based on these probabilities. In order to use the proposed P-BTD algorithms in simple readers with limited computational capabilities, all

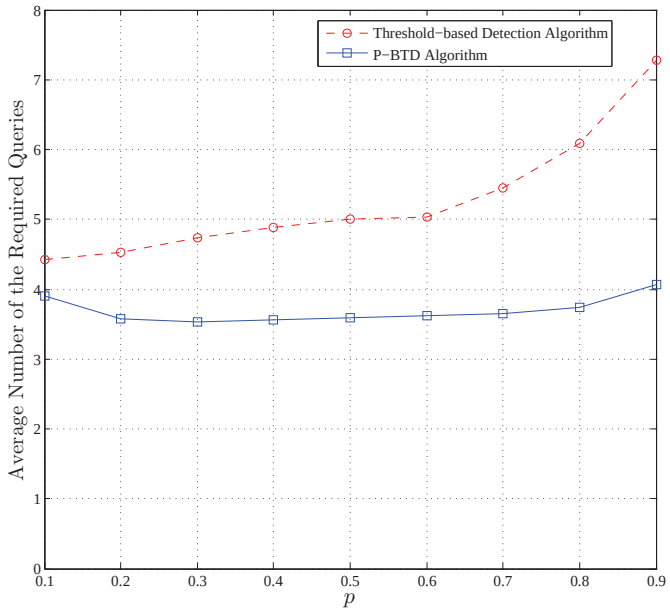

Figure 2.14: Average number of the required queries with inaccurate values of p (± 0.05 error) in the P-BTD and threshold-based algorithms. ($N = 500$, $h = 1$ and $T = 21$)

the probabilities can be calculated once and saved in a look up table (LUT). Basic readers can use this LUT to prevent the calculations required for the P-BTD algorithms.

We showed via simulations that the probabilities of false alarm are very low, in the order of 10^{-4}, for both the proposed binary tree walking and ALOHA-based P-BTD algorithms. It was also shown that the probability of missing the presence of a blocker tag in the system is zero for the proposed P-BTD algorithms. Based on the simulation results, the proposed P-BTD algorithms expedite the blocker detection procedure by reducing the number of required interrogations. Our proposed P-BTD algorithms have better performance than the threshold-based method because they use the probabilistic model of the blocker attack and continuously update the information about the system. The threshold-based method, on the other hand, relies on counting the number of RFID tags only and ignores other useful information such as the probabilistic behavior of the blocker attack. Sensitivity of the proposed P-BTD algorithms to inaccurate values of the input parameters was also

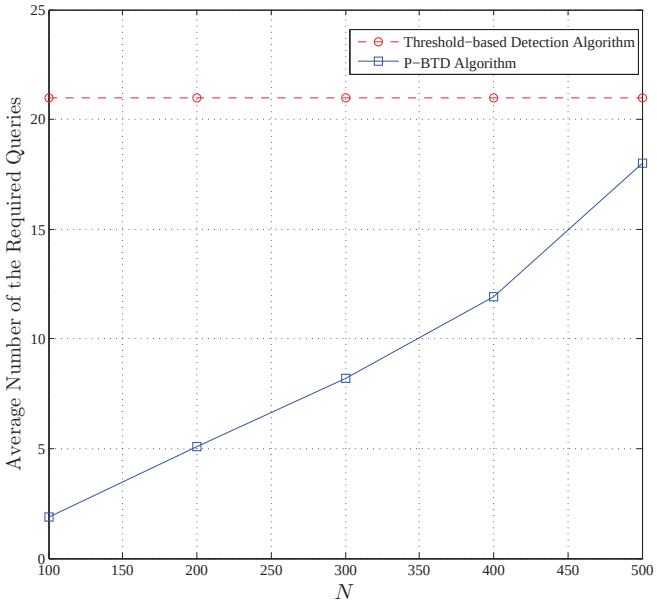

Figure 2.15: Average number of the required queries with inaccurate values of N ($\pm 5\%$ error) in the P-BTD and threshold-based algorithms. ($p = 0.7$, $h = 1$ and $T = 21$)

studied and it was shown through simulations that the proposed P-BTD algorithms can detect the presence of a blocker tag faster than the threshold-based method, even if the reader does not know the accurate values of N, F or p.

In order to design the P-BTD algorithms, we assumed that the reader may not have online access to a central database for checking the validity of the detected tag IDs. This is a reasonable assumption for many applications and readers. As explained in the example of the wine warehouse in Section 2.2.1.3, the reader may not know the ID of each tag at the beginning, but it knows how many bottles of wine have been transferred to the warehouse. At this stage, the reader only knows the number of tags present in the system but does not know their IDs. The reader (or the central database) will know the IDs after finishing the singulation procedure. Moreover, having online access to a central database can be a strong assumption for many applications [7]. Based on the above, we designed the P-BTD algorithms so that they do not rely on any previous knowledge of the tag IDs.

However, if the reader has online access to a central database and knows the IDs of the tags present in the system, then one line can be added to the proposed P-BTD algorithms (as an additional constraint) for checking the validity of each detected tag ID, without losing the generality of the proposed P-BTD algorithm.

Finally, the proposed analytical models for the binary tree walking and ALOHA singulation mechanisms were used to design probabilistic blocker tag detection algorithms in this study, however, these analytical models can also be used for many other purposes such as estimating the number of tags in an environment or improving the performance of RFID systems.

Chapter 3

Toward a Light-weight Authentication Protocol for RFID Systems

3.1 Introduction

RFID systems are vulnerable to security and privacy threats. Tracking customers, extracting personal information and selling illegally copied items are only few samples of these issues. To cope with security and privacy issues in RFID systems, various schemes have been proposed. These solutions can be divided into two general groups. The first group uses blocking, jamming and physical solutions for RFID security [45, 46, 47]. The other group uses cryptographic concepts and security protocols. Cryptographic solutions for RFID security issues can themselves be divided into two main groups, light-weight authentication protocols and complex cryptographic solutions. Some researchers believe that it is possible to use complex cryptographic protocols in future RFID tags. They believe the manufacturing costs of implementing cryptographic functions in RFID tags will decrease gradually and future RFID tags will have more computational power. Therefore, they suggest using public key solutions such as elliptic curve cryptography (ECC) [39, 42] and the advanced encryption standard (AES) [43]. Most RFID researchers, on the other hand,

believe that the industry needs simple and low cost RFID tags (below 5 cents per item) with limited number of logical gates [12, 97]. For this case, many approaches that are based on light-weight authentication protocols have been suggested [4, 5, 6, 7, 30, 32, 35, 37].

Light-weight authentication protocols have the advantage of keeping the computational demand and the price of RFID tags very low. For this reason, light-weight authentication protocols have been of interest to both industry and academia. In this work, we perform the security analysis of the EPC Gen-2 protocol as one of the major standards of communication between the tags and the reader in passive RFID systems. We also perform the security analysis of five other light-weight RFID protocols proposed in [4, 5, 6, 7], and show that they are vulnerable to some security attacks. We then propose a new light-weight authentication protocol that takes the hardware limitations and the manufacturing costs of RFID tags into consideration. The main goal of the proposed light-weight authentication protocol is to improve the security and reliability of communications between the tags and the reader(s) in RFID systems. We show that our proposed authentication protocol improves the level of security by solving the security issues of the protocols introduced in [4, 5, 6, 7]. Briefly, the contributions of this chapter are as follows:

- We perform the security analysis of the standard EPC Gen-2 protocol, as well as the light-weight authentication protocols proposed by Henrici and Müller [5], Lim *et al.* [6], Tan *et al.* [7] and Sun *et al.* [4], and show how they are vulnerable to simple attacks by malicious users.

- Using what we learned from the security issues of the above mentioned protocols and taking advantage of the SQUASH message authentication method [98], we propose a new light-weight authentication protocol that increases the security of communications between the readers and the tags in RFID systems.

- The computational cost and the complexity of the above mentioned protocols are

discussed and compared.

The rest of this chapter is organized as follows: Section 3.2 explains the standard EPC Gen-2 protocol [3] along with five recently proposed light-weight authentication protocols [4, 5, 6, 7]. Section 3.3 summarizes the security drawbacks of the explained protocols and shows some simple tricks that can be used by attackers to affect the normal function of these protocols. In Section 3.4, we propose a new light-weight authentication protocol that improves the security and privacy of the RFID protocols studied in Section 3.2. Finally, the security of the proposed protocol and its computational costs are compared with the discussed schemes in Section 3.5.

3.2 Related Works

3.2.1 EPC Class-1 Gen-2 RFID Protocol

The EPCglobal class-1 generation-2 (briefly EPC Gen-2) protocol was approved as the ISO 18000-6C standard in July 2006. This protocol was designed based on the specifications and limitations of a standard class of passive RFID tags called the EPC Gen-2 tags. A typical EPC Gen-2 tag contains a pseudorandom number generator (PRNG) and takes advantage of a cyclic redundancy code (CRC-16) to protect the message integrity during communication [3, 4]. An EPC Gen-2 tag gets its power from the reader, therefore, its computational power is limited. As a result, EPC Gen-2 tags cannot perform complex computations. In the EPC Gen-2 protocol, the communication process is performed as shown in Fig. 3.1:

1. First, a request message is sent from the reader to the tag (in the form of “Query”, “QueryAdj” or “QueryRep” commands) to start the session [3, 4].

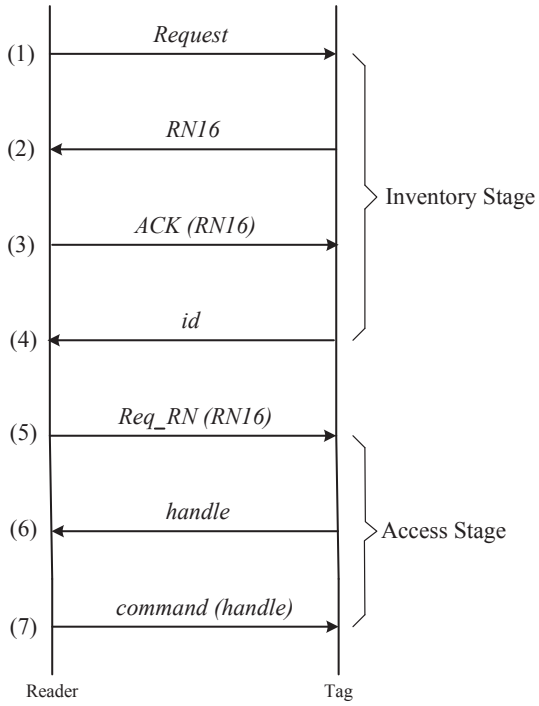

Figure 3.1: The standard EPC Gen-2 protocol [3, 4].

2. The tag responds to the request message by generating a random 16-bit string, denoted by $RN16$.

3. The reader sends an acknowledge message, $ACK(RN16)$, to the tag and waits for its response.

4. After receiving the $ACK(RN16)$, the tag sends its id in plain text to the reader and the session is terminated.

The above four steps are used for everyday RFID applications and called the "inventory stage". To modify all or part of the information stored in the tag, the reader can start another stage, denoted as the "access stage", (steps 5 to 7 in Fig. 3.1). In order to start the access session, the reader sends a $Req\_RN(RN16)$ message (containing the previous $RN16$) to the tag and asks it for another random number. The tag checks if the previous

RN16 is correct and then replies with a "handle" as explained in the EPC Gen-2 protocol. Finally, step (7) provides the appropriate memory access commands, such as "Read", "Write" and "BlockWrite" [3, 4]. The reader needs to provide the same handle as the one it received from the tag in step (6).

The EPC Gen-2 protocol only relies on the capabilities of EPC Gen-2 tags (PRNG and CRC-16 circuitries) and does not need additional hardware equipments (which increase the manufacturing price of RFID tags). Moreover, the reader can query a tag as much as it wants without worrying about the denial of service (DoS) issue. In addition to the EPC Gen-2 protocol, several light-weight authentication protocols have been proposed in recent years. The main purpose of these light-weight authentication protocols is to improve the security and privacy of the communications between the tags and the readers in RFID systems. In this section, we explain five recently proposed light-weight RFID protocols. We will explain how each of these protocols can be attacked by malicious users later in Section 3.3.

3.2.2 Henrici-Müller RFID Protocol

The protocol proposed by Henrici and Müller is a simple communication scheme designed for RFID systems [5]. It relies on one-way hash functions and aims to prevent the tracking attack by changing the traceable data at each interrogation. A hash function is generally defined as an algorithm or subroutine that maps large data sets of variable length to smaller data sets of a fixed length. In Henrici-Müller protocol, it is assumed that the singulation procedure has been accomplished by the reader previously. Singulation is a method used by RFID readers to identify which tags are present in the system [20, 45]. The principles of this protocol are as follows: after the singulation phase, each tag contains its current identifier id, the current session number i, and the last successful session number i^*. Similarly, the

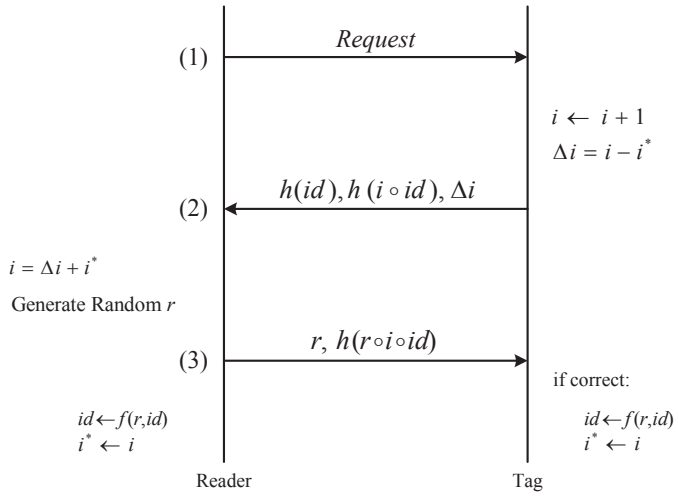

Figure 3.2: The RFID protocol proposed by Henrici and Müller [5].

database contains a list of all identifiers, session numbers and the last successful session numbers for all the tags in the system. In addition to id, i and i^*, the list contains the hashed value of id, denoted by $h(id)$, for each tag in the system. In this scheme, both the reader and the tags are aware of the hash function h. At the very beginning, id and i are initialized with random values and i^* is equal to i. After initialization, the communication process is performed as shown in Fig. 3.2 and consist of the following steps:

1. First, a request message is sent from the reader to the tag to start the session.

2. After receiving a request message from the reader, the tag increases the value of its i by one and calculates $h(id)$, $h(i \circ id)$ and $\Delta i = i - i^*$, and sends them to the reader via the insecure wireless channel. Here, $\circ$ is a "suitable conjugation function" as mentioned in [5].

3. The reader sends the above information to the database. The database calculates the hash functions for all the tags in the system and finds the tag whose id results in the received hash value $h(id)$. The database extracts i^* of the tag and calculates

i ($i = i^* + \Delta i$) and i^*. The database calculates $h(i \circ id)$ and checks whether or not it matches the one sent by the tag. If the tag is confirmed by the database, a random value r is generated. Then, r and $h(r \circ i \circ id)$ are sent to the tag.

4. Since the tag knows i and id and it receives r from the reader, it can calculate $h(r \circ i \circ id)$ to make sure that it is communicating with the legitimate reader. If this is the case, the tag calculates its new identifier using a predefined function of the received r like $f(r, id)$, and updates the last successful session number i^* which is set to i.

It should be noted that in this protocol, an entry is not deleted from the database even after the third step, but a copy of the previous id and i^* are kept until the next successful session. If the third step fails for any reason or the tag cannot receive the random value r correctly, the database can still identify the tag using the previous id and i.

3.2.3 Lim *et al.* RFID Protocols

Here, we explain two RFID protocols proposed by Lim *et al.* [6]. These protocols have been designed to improve the security of communication in RFID systems and to provide a more reliable solution than [5]. The first protocol proposed by Lim *et al.* is named the "challenge-response trigger" and uses a challenge-response mechanism to provide the required security for RFID systems. After the singulation phase, each tag contains its current id, and a copy of all the tag ids is kept in the database as well. The communication process is performed as shown in Fig. 3.3:

1. First, a request message is sent from the reader to the tag, along with a random challenge R to start the session.

2. The tag generates a random challenge R' after receiving the request from the reader

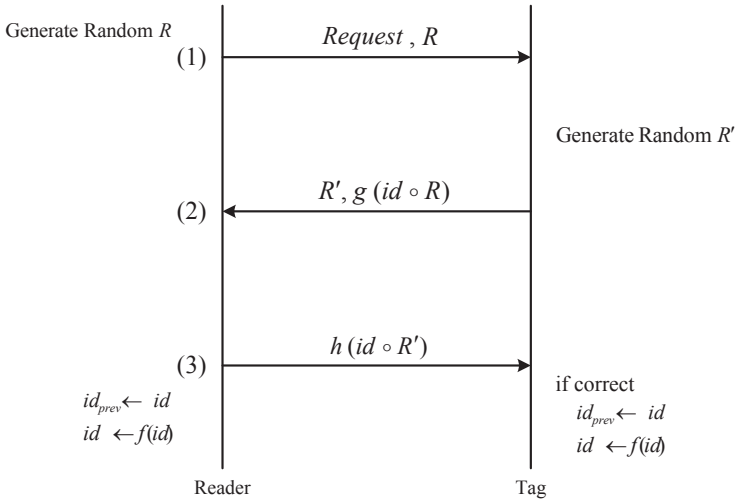

Figure 3.3: The challenge-response trigger protocol proposed by Lim *et al.* [6].

and sends it along with the $g(id \circ R)$ value to the reader. Again, $\circ$ is a "suitable conjugation function" like XOR, and g is a one-way hash function [6]. The tag uses the received R in its response $g(id \circ R)$ to convince the reader that it is communicating with the legitimate tag, and not with an attacker.

3. The reader forwards the information in step (2) to the database and the information is checked there. If $g(id \circ R)$ is correct, the database calculates $h(id \circ R')$ and sends it to the tag via the reader. Like g, h is also a one-way hash function. The new id is calculated using a function f which is known by both the tag and the database.

It should be noted that in the challenge-response trigger protocol, an entry is not deleted from the database after the third step, but a copy of the previous id is kept until the next successful session. If the third step fails for any reason, the database can still identify the tag using the previous id. After introducing the challenge-response trigger approach, another protocol was proposed by Lim *et al.* to improve the security of reader-tag communication in RFID systems. This scheme is named the "forward rolling trigger" protocol and takes advantage of the Lamport's one-time password authentication scheme [99]. In

this scheme, the tag only responds to a valid challenge from the reader, otherwise it sends back some random value [6]. In the forward rolling trigger protocol, the reader stores a chain of hash functions $h(w)$, $h^2(w)$, $h^3(w)$,..., $h^{max}(w)$, where h is a secure one-way hash function, w is a secret random seed, and max is the length of the chain. For each tag in

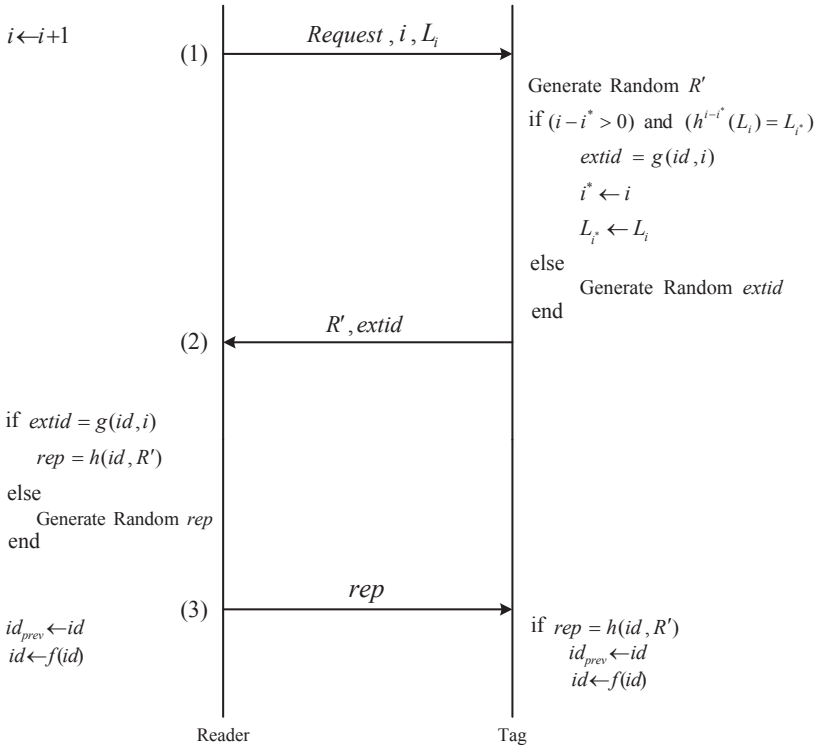

Figure 3.4: The forward rolling trigger protocol proposed by Lim *et al.* [6].

the system, the last successful session (communication with the reader) is stored as i^* and the current session is indicated by i. The reader uses $L_i = h^{max-i}(w)$ to authenticate itself to the tag. The values of i^* and i are initialized to 0 at the beginning, and L_i is initialized to $h^{max}(w)$. The communication process is shown in Fig. 3.4 and has the following steps:

1. The reader sends i and L_i to the tag, along with the request message, to start a new session with the tag.

2. The tag checks whether $(i - i^*)$ is greater than 0 and $h^{i-i^*}(L_i)$ is equal to L_{i^*}. If these

two conditions hold, it calculates $extid = g(id, i)$, in which i is the current session number and id shows the identification of the tag. It also updates i^* to be i, L_{i^*} to be L_i, generates a random challenge R', and sends the $extid$ and R' to the reader. The tag replies to the reader's request with a meaningless random value instead of $extid$ if any of the two mentioned conditions does not hold.

3. The reader forwards the received information to the database and if the received $extid$ is correct, $rep = h(id, R')$ is calculated and sent to the tag via the reader. Otherwise, a meaningless random rep is generated and sent to the tag.

4. After sending the rep to the tag, the current id is stored as the previous identification id_{prev} and the new id is calculated using $f(id)$ in which f is a one-way function known by the tag and the reader. At the tag side, id_{prev} and id are updated only if the received rep is equal to $h(id, R')$.

It should be noted that as in the previous three protocols, an entry is not deleted from the database after the third step, but a copy of the previous id is kept until the next successful session. If the third step fails for any reason, the database can still identify the tag using the previous id.

3.2.4 Tan *et al.* RFID Protocol

The majority of recent RFID protocols such as the EPC Gen-2 standard and the protocols proposed in [5] and [6] take advantage of a central database to store the RFID tag data. In these schemes, the reader queries the tags and sends the information to a central database using a secure line. After authentication, the database returns the tag data to the reader. In [7], however, Tan *et al.* proposed a novel server-less authentication protocol that aims to provide the same level of security as the previous protocols without needing a central

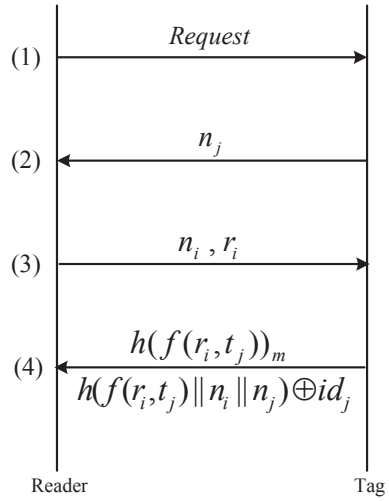

Figure 3.5: The server-less protocol proposed by Tan *et al.* [7].

database. In this scheme, each reader has a unique identifier r_i and each tag has a unique identifier and a unique secret t_j. For each tag, the secret t_j is only known by the tag and a central database. A one-way hash function h is known to all the tags and the readers. Let $f(a, b) = h(a||b)$ in which $||$ is the concatenation operation and a and b are the arguments of f. Each reader r_i is connected to the central database only once at the initialization step and receives $f(r_i, t_1)$ for the first tag, $f(r_i, t_2)$ for the second tag, ..., and $f(r_i, t_n)$ for the n-th tag in the system. It should be noted that the reader does not have access to the secret t_j of the j-th tag, but it knows the hash function $f(r_i, t_j)$ [7]. Detail of the server-less protocol is shown in Fig. 3.5 and it works as follows:

1. The reader first sends a request message to the tag.

2. The tag replies to the request from the tag by sending a random challenge n_j.

3. The reader sends its identifier r_i along with a random challenge n_i to the tag.

4. The tag calculates $h(f(r_i, t_j))$ and sends its first m bits, denoted by $h(f(r_i, t_j))_m$ to the reader. In addition to $h(f(r_i, t_j))_m$, the tag calculates $h(f(r_i, t_j)||n_i||n_j) \oplus id_j$

and sends it back to the reader, where $\oplus$ is the XOR operation.

5. The reader checks its database and calculates the hash function of all of its entries $f(r_i, t_j)$, and looks for the candidates that match the first m bits of $h(f(r_i, t_j))_m$. If there is a match, the reader uses the random challenges n_i and n_j to obtain $h(f(r_i, t_j)||n_i||n_j)$, and then, calculates id_j using an XOR operation.

This protocol is easy to implement, inexpensive, and does not rely on the back-end database concept. Moreover, it has been shown that this protocol can resist the DoS, cloning, replay and physical attacks [7]. However, it has some security issues which will be explained in Section 3.3.

3.2.5 Sun *et al.* Gen-2^+ RFID Protocol

Here, we discuss the Gen-2^+ protocol proposed by Sun *et al.* [4]. As mentioned in Section 3.2.1, the EPC Gen-2 protocol is inexpensive and easy to implement, however, it does not provide a secure protocol for communication between the legitimate readers and the tags. The *id* is sent in plain text to any reader who queries and sends an acknowledge message to the tag. This can jeopardize the privacy of the RFID technology consumers. Based on the above, Sun *et al.* modified the EPC Gen-2 protocol so as to provide mutual authentication between the legitimate readers and the tags. The modified version of the EPC Gen-2 protocol is named the Gen-2^+ protocol. It uses the PRNG and CRC-16 tools which are predicted in the EPC Gen-2 standard. Sun *et al.* assumed that each tag shares an l-word-long random string, called "key-pool", with the back-end database. This string is randomly generated by the back-end database and is written into the tag before deployment [4]. A threshold t is also set in each tag to tolerate errors in the received bits and to boost the reading speed. Up to this point, no additional circuitry was needed by the Gen-2^+ protocol. However, Sun *et al.* assumed that it is possible to design and add an

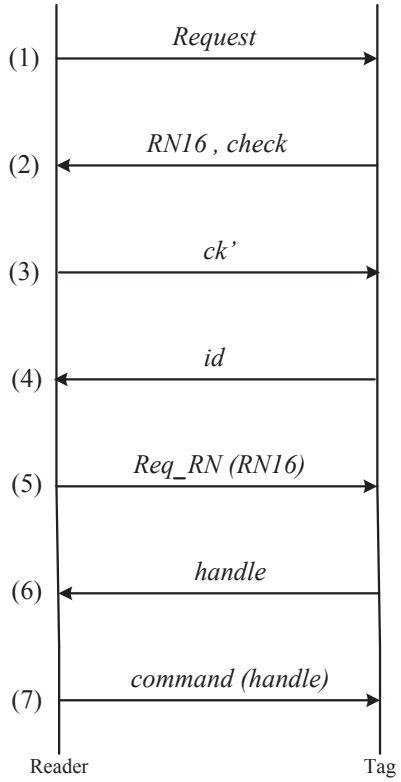

Figure 3.6: The Gen-2^+ protocol proposed by Sun *et al.* [4].

extra Hamming distance calculator to each EPC Gen-2 tag [4]. The Gen-2^+ protocol is depicted in Fig. 3.6 and works as follows:

1. A request message in the form of Query, QueryAdj or QueryRep [3, 4] is sent from the reader to the tag.

2. The tag generates a 16-bit random number $RN16$ using its PRNG circuitry and sends it to the tag. It also sends a *check* message that provides two bits of additional information about the tag. In this scheme, the 16-bit $RN16$ is divided into two 8-bit binary strings, called a and b. The *check* message is calculated by performing the XOR operation on the last two bits of a and b, i.e. $a_6 \oplus b_6$ and $a_7 \oplus b_7$, and it is used to boost the process required for identifying the tag [4].

3. The reader sends the $RN16$ (composed of a and b) and the *check* values to the back-end database. The database searches the key-pool to find the 16-bit key which is pointed out by a and b. This key is denoted by ck' and it is sent to the tag by the reader.

4. The tag compares this ck' with its key ck to see if their Hamming distance is less than the threshold t. The tag accepts the reader as a legitimate reader and sends its id if the mentioned Hamming distance is less than t, otherwise, it does not send its id and waits for a new ck' from the reader which is close enough to ck.

These four steps are usually enough for common RFID applications. However, steps (5) to (7) can be used by the reader as explained in Section 3.2.1, to modify all or part of the tag's information or to access its memory [3, 4]. This protocol is very similar to the EPC Gen-2 protocol discussed in Section 3.2.1, except that the security of communications between the readers and the tags is increased in Gen-2^+ by using an extra circuitry for calculating the Hamming distance between two binary strings. There is also another cost for the increased security of the Gen-2^+ protocol compared to the EPC Gen-2 protocol, and that is the high number of queries required to identify a communicating tag by a legitimate reader. It has been shown in [4] that approximately 15 queries are needed (on average) to identify a tag using the Gen-2^+ protocol.

3.3 Security and Privacy Issues

Although the protocols discussed in Section 3.2 are easy to implement and inexpensive, they are vulnerable to some attacks. We first define these attacks and then show how a malicious user can exploit them to interrupt each of the protocols discussed in Section 3.2. Below is a list of some simple and common attacks that can be carried against RFID

systems:

- Tracking: under this attack, a malicious user who can passively eavesdrop on the communication between the tags and the readers or can actively interact with the tags, tries to trace a specific tag or to identify it among numerous tags, using the information sent by the tag over time.

- De-synchronization: the main goal of this attack is to ruin the synchronization between a legitimate reader and a tag, in order to prevent them from successfully communicating with each other. Moreover, this attack can be carried to prevent the reader from successfully updating the information (identification for instance) of a tag after a successful communication.

- Replay: under this attack, a malicious user eavesdrops on the communications between a legitimate reader and a tag and saves the information sent by them. The attacker uses this information later, i.e., it replays the saved information to communicate with a legitimate reader or a real tag.

- Denial of Service (DoS): the aim of this attack is not to obtain information about a specific tag, but rather to ensure that a legitimate reader cannot communicate with this tag any more. In order to launch this attack, the adversary needs to waste (use) some resources of the tag (or reader) which are necessary for their communication.

- Impersonation: the objective of this attack is to obtain the information sent by a tag and a legitimate reader during their communication. This information is then used by a fake tag to convince the legitimate reader that it is communicating with a specific real tag, and not a fake one.

3.3.1 EPC Class-1 Gen-2 RFID Protocol

The main advantage of the Gen-2 protocol is that it only relies on the capabilities of the EPC Gen-2 tags (PRNG and CRC-16 circuitries) and does not need additional hardware equipments which increase the price of manufacturing RFID tags. Moreover, the reader can query a tag as much as it wants without worrying about the denial of service (DoS) issue. However, this protocol is vulnerable to some security threats. Using the above definitions, some of the security drawbacks of the Gen-2 protocol are explained below:

1. Revealing the information: any reader who can receive the RN16 message is able to convince the tag to send its data in plain text by transmitting the $ACK(RN16)$ message to the tag. Therefore, the Gen-2 protocol jeopardizes the costumers' privacy by revealing the information about their tag items.

2. Tracking: it is possible to track a specific tag (and the costumer carrying that item) as the *id* is static and does not change over time. Therefore, any malicious reader can send the request message repeatedly and look for the tag that replies with the expected *id*.

3. Replay and Impersonation: any malicious reader can eavesdrop on the communication between a real tag and a legitimate reader. This information can be stored on a fake tag and "replayed" so as to mislead a legitimate reader or to "impersonate" itself as the real one.

4. De-synchronization: if a legitimate reader wants to obtain information about a tag, it sends the request message to the tag and this should be followed by the $RN16$ reply from the tag. Now assume that an attacker sends another request message to the tag after step (2). The attacker forces the tag to generate another $RN16$ this way. The legitimate reader replies with the $ACK(RN16)$ containing the previous

$RN16$ while the tag is expecting an $ACK(RN16)$ containing the new $RN16$. This way, the attacker corrupts the synchronization between the tag and the legitimate reader. As a result, the tag does not reply to the received $ACK(RN16)$ from the legitimate reader and the communication fails.

3.3.2 Henrici-Müller RFID Protocol

This protocol is simple, efficient, and can solve many security issues of RFID systems, however, it is vulnerable to some simple attacks that may jeopardize the privacy of RFID users. Below, we explain some of the security drawbacks of this protocol:

1. Tracking (type I): In the Henrici-Müller protocol, every time the tag receives a request message, it increases the value of i by one, even if the session finally fails. However, i^* is updated only if the session is successful and the reader is confirmed. Based on the above, an attacker can interrogate a tag several times to abnormally increase i and Δi. As can be seen in Fig. 3.2, Δi is sent to the reader in the second step. Therefore, an attacker is able to recognize its target by identifying and tracking the tag which sends abnormally large values of Δi in response to requests by the attacker.

2. Tracking (type II): An attacker can repeatedly send the request message to the nearby tags and looks for the $h(id)$ in the received replies. The attacker can track a specific tag using its $h(id)$ as it does not change over time. The tag remains vulnerable to the tracking attack until a successful session is accomplished and its id is updated.

3. De-synchronization (type I): After step (2) and before the legitimate reader sends r and $h(r \circ i \circ id)$ to the tag, the attacker can send its own r' and $h(r' \circ i \circ id)$ to the tag. The attacker does not know i and id separately but it knows $h(i \circ id)$ from the tag's response in step (2). Therefore, the attacker can simply use the null element

($r' = \bar{0}$) and send back the r' and $h(r' \circ i \circ id)$ to the tag. As a result, the original r and $h(r \circ i \circ id)$ will not be accepted from the legitimate reader and it will be desynchronized from the tag.

4. De-synchronization (type II): In Henrici-Müller protocol, when the legitimate reader is interrogating a tag, the attacker can interrogate this tag before the reader carries out the third step. After receiving the request message from the attacker, the tag increases i by one. Consequently, the hash value sent by the legitimate reader to the tag is conceived as an incorrect response and will not be accepted (since the tag expects to receive a hash value calculated from the newly increased i).

5. Replay and impersonation: As mentioned before, a copy of the previous id is kept in the database, so it is possible for the reader to communicate with a tag whose id has not been updated for any reason. Using this fact, an attacker can simply save and then replay $\{h(id), h(i \circ id), \Delta i\}$ to the legitimate reader to impersonate itself as the real tag.

3.3.3 Lim *et al.* RFID Protocols

The challenge-response trigger protocol proposed by Lim *et al.* can be attacked using some simple tricks. Below, we explain some of the security drawbacks of this protocol:

1. Replay and impersonation: for many RFID applications, it is a reasonable assumption that a tag may be captured and analyzed by an attacker. The attacker can interrogate the captured tag for some values of R, and make a dictionary of these challenges and the corresponding responses from the tag. The attacker can use this dictionary later to masquerade and impersonate itself as the real tag for the legitimate reader.

2. Tracking: the above mentioned dictionary can be used to track a specific tag. In

order to do that, the attacker would repeatedly send the request message and a known challenge R to nearby tags, and look for the corresponding $g(id, R)$ among the received responses (which is known from the dictionary). The tag remains vulnerable to the tracking attack in the challenge-response trigger protocol until a successful session is accomplished and its id is updated.

3. De-synchronization: after sending the request message from the legitimate reader to the tag in step (1) and before step (3), an attacker can repeat step (1) and send another request to force the tag to reset the random challenge R'. This new random challenge would be different from the previous one, which was sent to the legitimate reader. Therefore, the $h(id \circ R')$ message which is made from the first challenge will not be accepted by the tag. The reader wrongly assumes that the id has been updated using the function f after sending $h(id \circ R')$ in the third step.

As in the case of the challenge-response trigger protocol, the forward rolling trigger protocol has some security issues that may affect the privacy of RFID users. Below, we explain some security drawbacks of this protocol:

1. Limited number of sessions: for each tag, the total number of session requests that can be issued by the reader is limited to max, due to the fact that any i from the set $\{1, 2, 3, ..., max\}$ can be used only once (for each tag). This limit applies to the case when the reader knows exactly which tag should be interrogated next. For example, assume that the reader has used $i = 8$ and L_8 for tag A, and $i = 3$ and L_3 for tag B, in its most recent interrogations with these tags. If the reader knows that it is going to interrogate tag A in the next session, any i from the set $\{9, 10, 11, ..., max\}$ can be used to start the new session (as it had used $i = 8$ and L_8 in the previous session with tag A). For tag B, however, any i from the set $\{4, 5, 6, 7, 8, 9, ..., max\}$ can be used if the reader knows it is going to interrogate tag B in the next session

(as it had used $i = 3$ and L_3 in the previous session with B). This is the best scenario in which every i from the set $\{1, 2, 3, ..., max\}$ can be used for each tag. However, the reader does not always know which tag is going to be interrogated in the next session. For example, in an RFID-based library, the reader should start the session first and wait for the RFID tag to answer and reveal its id [21]. For this type of applications, the reader has to increment i at each interrogation, therefore, the total number of sessions for all tags (not each tag) is limited to max.

2. DoS attack: the attacker may know the set of acceptable $\{i, L_i\}$ pairs (or a large pair of this set) from another RFID system or by tampering. In that case, the attacker can send $i = max$ and L_{max} to a tag and waste its previous pairs. This way, the tag loses its chance for communication with the legitimate reader in future sessions because the condition $(i - i_{tag}) > 0$ is not satisfied anymore.

3. De-synchronization: the $(i - i_{tag}) > 0$ condition makes the protocol vulnerable to DoS attack as explained above. Moreover, the reader needs to be aware of the tag which is going to be interrogated next, and this is not a plausible assumption for many applications. On the other hand, if we remove the $(i - i_{tag}) > 0$ condition, the protocol becomes vulnerable to de-synchronization and tracking attacks. The attacker may listen to the communications between the tags and the reader in another RFID system, eavesdrop and save a valid (i, L_i) pair, and use it for an RFID system somewhere else. For example, a legitimate reader may send a request along with an acceptable (i_1, L_{i_1}) pair to a tag and the tag replies with $\{R'_1, extid_1 = g(id, i_1)\}$. At this stage and before sending the rep message from the reader to the tag, an attacker can send another request with another acceptable (i_2, L_{i_2}) pair to force the tag to reply with $\{R'_2, extid_2 = g(id, i_2)\}$ and this way, it ruins the synchronization between the tag and the reader.

4. Tracking: if we eliminate the $(i - i_{tag}) > 0$ condition to prevent the DoS attack, an attacker can eavesdrop on the previous communications between the tag and the reader and use one of the previously used valid (i, L_i) pairs to interrogate the tag again. The tag replies with $extid = g(id, i)$ and the attacker can track the tag by sending the request message repeatedly and tracking the tag which replies with $extid = g(id, i)$. In other words, $extid = g(id, i)$ is a static information and it can be used to track a tag before the third step (in which id is updated and $extid = g(id, i)$ is changed).

5. Impersonation: an attacker can eavesdrop on the communication between a legitimate reader and a tag, and extract a valid (i, L_i) pair and its corresponding $extid$. Using the valid pair of (i, L_i) and $extid$, and considering the fact that a copy of the previous id and i^* is kept by the reader until the next successful session, it is possible for the attacker to impersonate itself as a legitimate tag if the (i, L_i) pair is used again by the reader (for interrogating other tags for instance).

3.3.4 Tan *et al.* RFID Protocol

This protocol is easy to implement, inexpensive, and does not rely on the database concept. Moreover, it has been shown that this protocol can resist the DoS, cloning, replay and physical attacks [7]. However, it has some security issues which may be exploited by an attacker as shown below:

1. De-synchronization: a malicious user can send a request message to the tag after step (3) and force it to generate a new challenge n'_j. At this point, the reader waits for $h(f(r_i, t_j))_m$ and $h(f(r_i, t_j)||n_i||n_j) \oplus id_j$ while the tag is expecting a new n'_i and r_i as the third step. This way, the synchronization between the tag and the reader is corrupted and the session ends uselessly.

2. Tracking: in step (4) of the explained scheme, $h(f(r_i, t_j))_m$ is a static form of data which can be used by malicious users to track the tag. Using this information, the attacker can find a specific tag among the other tags by repeatedly sending the request message with a fixed r_i and looks for the tag which replies with $h(f(r_i, t_j))_m$.

3. Impersonation: it is possible that an attacker captures a tag, repeatedly sends the request message along with fixed values of r_i and n_i, and then stores the $\{h(f(r_i, t_j))_m$, $h(f(r_i, t_j)||n_i||n_j) \oplus id_j\}$ responses received for different values of n_j. This procedure is then repeated by changing the value of n_i. The attacker can make a table of the responses for some values of n_i and n_j, and make a fake tag to impersonate it as a real one for a reader with r_i.

3.3.5 Sun *et al.* Gen-2^+ RFID Protocol

The Gen-2^+ protocol is designed based on the capabilities of the standard EPC Gen-2 RFID tags. Therefore, it does not require any modification in the hardware architecture of the tags. It is easy to implement and inexpensive. However, the Gen-2^+ protocol has some security problems as follow:

1. Tracking: To obtain the *id*, an attacker needs to be able to provide an acceptable ck' and *check* for each $RN16$ it receives in step (2). It is proven in [4] that if an attacker records approximately 16,384 failed sessions between a reader and a tag and analyses them, it may be able to track the tag using the additional information provided by the *check* bits during the past 16,384 failed sessions. Moreover, a passive attacker can listen to the communication between the legitimate readers and the tags, and notice the presence of a specific tag, as the *id* is sent in plain text in the Gen-2^+ protocol.

2. Impersonation and replay: An attacker can eavesdrop on the communication between a legitimate reader and a tag, and extract its id, $RN16$ and $check$. The attacker can save this information on a fake tag. The fake tag then accepts any ck' it receives from the reader and sends its id in step (4) to impersonate itself. It should be noted that this attack is possible as long as the key-pool does not get updated by a legitimate reader.

3. De-synchronization: An attacker can wait until a tag is interrogated by a legitimate reader and sends its $RN16$ and $check$ in step (2). At this point and before the legitimate reader calculates ck' and sends it to the tag, another request message can be sent to the tag by the attacker. This way, the tag replies with another $RN16$ (or equivalently with another a and b) which points to a different location in the key-pool. As a result, the tag does not accept the ck' which was sent by the legitimate reader. In other words, the Gen-2^+ protocol is vulnerable to de-synchronization attack.

3.4 The New Light-weight Authentication Protocol

In Section 3.2, we showed that none of the protocols proposed in [4, 5, 6, 7] are completely secure, and explained how each of these protocols can be attacked. We also discussed about the hardware limitations of RFID tags, and explained why sophisticated encryption methods are not appropriate for many RFID applications. After analysing the security drawbacks of the studied protocols and using what we learned from this study, we propose a new protocol in this section that provides a higher level of security for RFID communication. In order to make the proposed protocol appropriate for real RFID applications, the limitations of the hardware architecture and the cost of implementing RFID tags should be taken into account as well. To address the hardware limitations of RFID tags, we take

advantage of the SQUASH message authentication method proposed by Shamir [98], and use it as the method of hash function calculation in our proposed protocol. The SQUASH method not only provides an inexpensive way of calculating the hash functions needed for our protocol, but also improves the level of security in the proposed protocol, as we will explain it later in Section 3.4.1.

3.4.1 Why the SQUASH Method?

Most of the recently proposed light-weight authentication protocols (including the protocols discussed in Section 3.2) use a one-way hash function h to provide the required secrecy for the RFID protocols. However, there exist some strict limitations on the hardware architecture and the price of each manufactured tag that have rarely been considered and addressed in recent works. It has been suggested that the price of each manufactured tag should be less than 5 cents to be acceptable for the industry [12], and the final manufacturing price depends on the number of gates used in each tag. There are many hash functions and security protocols that provide very high level of security, however, implementing these functions on RFID tags increases the number of required gates and as a result, the price of the tags increases. As an example, the zero knowledge (ZK) interactive protocols are able to prevent any leakage of information about the secret data, but they are too complicated for RFID tags [98]. In other words, we cannot expect sophisticated calculations from RFID tags if we want to comply with the limitations on the architecture and the price of RFID tags. Considering the above facts, many of the current hash functions and cryptography tools are not suitable for RFID tags. Therefore, we need to design (or use) an RFID specific one-way hash function that takes the limitations of RFID systems into account and provides the required security at the same time [100]. To address the hardware limitations of RFID tags while providing the required security and privacy, some specifically designed

hashing and encryption functions have been proposed in recent years. We can mention Hummingbird [101, 102, 103], GRAIN-128 [104], QUARK [105] and SQUASH-128 [98] as some of the best encryption schemes specifically designed for RFID tags.

For RFID protocols, we need a one-way hash function h which can combine two pieces of information, the secret S and the non-secret NS information, and protect the secrecy of S. This function must be able to hide S, but should not necessarily be a collision-resistant function since the discovery of a collision is not a security threat for challenge-response RFID protocols. However, most of the standard hash functions, such as SHA-1, have been designed to resist collision attacks and prevent forgery of digitally signed documents. This is a very difficult requirement to satisfy and adds a lot of unnecessary complexity to the hardware implementation of the hash functions, making them too complicated for RFID tags. Finally, the hash function used for RFID applications should not depend on an internal source of random bits. Considering the above facts, Shamir proposed a new hash function, called SQUASH, which is ideal for challenge-response protocols in highly constrained devices like RFID tags [98]. The SQUASH function is completely deterministic, rather than probabilistic. Moreover, it can be easily implemented for different word sizes and does not need random bit generators. In addition to ease of implementation and hardware architecture, it has been proven that the SQUASH method is at least as secure as Rabin's [106] public key encryption scheme, which has been investigated for more than 30 years [98]. A reduced version of the SQUASH method, named SQUASH-128, has been suggested in [98] for RFID applications. In SQUASH-128, the hash function has two 64-bit inputs (as S and NS), and generates a 32-bit hash value as the output. The public key which is used in SQUASH-128 is $n = 2^{128} - 1$. We take advantage of the SQUASH-128 method and use it as the hash function in our proposed light-weight authentication protocol.

3.4.2 Reduced Version of the SQUASH

Considering the hardware and price limitations of RFID tags, Shamir modified the general SQUASH scheme and designed an RFID-based hash function called SQUASH-128 [98]. In fact, the SQUASH-128 is a reduced version of the SQUASH method. For simplicity, we use the word SQUASH to refer to the general SQUASH scheme in this chapter. The SQUASH-128 scheme does not need any source of randomness and there is no way a legitimate tag fails to convince a legitimate reader that it is authentic. The SQUASH-128 scheme is capable of protecting privacy of the secret information S, even if the attacker has access to $h(S, NS_i)$ for many known or chosen NS_i. Below, we explain how the SQUASH and SQUASH-128 schemes can be implemented.

Actually, the SQUASH method simplifies and speeds up the Rubin's encryption scheme, and the SQUASH-128 is a modified and reduced version of the SQUASH scheme. The basic idea of SQUASH (and of course SQUASH-128) is to calculate a good approximation of the ciphertext produced by Rabin's encryption scheme, in a short window of bits (binary sequence representing the value that we want to calculate its hash). The SQUASH scheme works based on the following equation:

$$c \equiv m^2 \bmod n \tag{3.1}$$

where m is the message to be encrypted (hashed), n is the key used for encryption and c is the ciphertext used for authentication. In the SQUASH method, a number of the form $n = 2^k - 1$ (called a Mersenne number) is used as the encryption key. This form of n can be stored very compactly because its binary representation only uses k bits of 1's. The Mersenne number of the form $n = 2^k - 1$ is not only easy to store, but also makes the computation of (3.1) pretty simple. Since $1 \equiv 2^k \bmod n$, we can only compute the double

sized m^2, and numerically add the lower half to the upper half of it to calculate (3.1). More precisely, if $n = 2^k - 1$ and

$$m^2 = m_U^2 \times 2^k + m_L^2 \tag{3.2}$$

where m_U^2 indicates the higher half of m^2 and m_L^2 shows the lower half of m^2, then

$$m^2 \equiv (m_U^2 + m_L^2) \bmod n. \tag{3.3}$$

For example, if m is equal to 5 (binary representation 101), then m^2 is equal to 25 (binary representation 011001). Therefore, $m_U^2 = 011$ and $m_L^2 = 001$. Assuming that $n = 7$ ($k = 3$), then $4 \equiv m^2 \bmod n$ which can be calculated by adding 011 and 001 in the binary form which results in 100.

The tag does not really need to send all the bits of c to the reader to authenticate itself. It has been shown that only 32 bits of c is sufficient for this purpose if the attacker has no prior information about the expected c [98]. Another useful point which can be used in implementing the SQUASH scheme is that the tag can compute the successive bits of m^2 without storing all bits of the m sequence from the beginning of calculation. Instead, two streams of bits can be convolved and generate the final m^2 bit by bit. The tag calculates bit j of m_L^2 by summing all the products of $m_v \times m_{j-v}$ for $v = 0, 1, 2, ..., j$ and adding the carry from the previous bit to this sum as below:

$$m_j^2 = \sum_{v=0}^{j} m_v \times m_{j-v} + r_{j-1} \tag{3.4}$$

where r_{j-1} shows the carry from the $(j-1)$-th bit. To calculate bit $j+k$ in the upper half of m^2, the tag sums the product of $m_v \times m_{j+k-v}$ for $v = j+1, j+2, ..., k-1$ and adds the

carry from the previous bit to this sum as below:

$$m^2_{j+k} = \sum_{v=j+1}^{k-1} m_v \times m_{j+k-v} + r_{j+k-1} \tag{3.5}$$

where r_{j+k-1} shows the carry from $(j+k-1)$-th bit [98]. In order to clarify the process required for calculating m^2_L and m^2_U, we consider the above mentioned example again ($m = 5$, $k = 3$, $n = 7$). Bits 0 to 2 of m^2_L is calculated using (3.4) as below:

$$j = 0 \;\; ; \quad m^2_0 = \sum_{v=0}^{0} m_v \times m_{-v} \equiv (1 + r_0) \bmod 2 \tag{3.6}$$

$$j = 1 \; ; \; m^2_1 = r_0 + \sum_{v=0}^{1} m_v \times m_{1-v} \equiv (0 + r_1) \bmod 2 \tag{3.7}$$

$$j = 2 \; ; \; m^2_2 = r_1 + \sum_{v=0}^{2} m_v \times m_{2-v} \equiv (0 + r_2) \bmod 2 \tag{3.8}$$

where $r_0 = 0$, $r_1 = 0$ and $r_2 = 1$. Similarly, bits 3 to 4 are calculated using (3.5) as below:

$$j + k = 3 \; ; \; m^2_3 = r_2 + \sum_{v=1}^{2} m_v \times m_{j+k-v} \equiv (1 + r_3) \bmod 2 \tag{3.9}$$

$$j + k = 4 \; ; \; m^2_4 = r_3 + \sum_{v=2}^{2} m_v \times m_{j+k-v} \equiv (1 + r_4) \bmod 2 \tag{3.10}$$

where $r_3 = 0$ and $r_4 = 0$. Therefore, $m^2_L = 001$, $m^2_U = 011$ and $m^2 = 011001$. When the

tag wants to calculate m^2 mod n (where $n = 2^k - 1$), it needs to sum the upper half and the lower half of m^2. In order to do that, the j-th bit c_j of $c \equiv m^2 \bmod n$ is calculated by adding bits j and $j + k$ of m^2, along with the carry bit.

SQUASH-128 is exactly the same as SQUASH, except that it uses $n = 2^{128} - 1$ ($k = 128$) as the encryption key. It gets a 64-bit S (id for example) and a 64-bit NS (challenge for example) and generates a 32-bit ciphertext. SQUASH-128 is more secure compared to Robin's scheme, and no efficient attack on it is known [98]. The best attack on SQUASH-128 (if possible) would require exponential time and grows monotonically with the size of n. Even finding the *complete* factorization of $n = 2^{128} - 1$ (if possible) does not necessarily make the SQUASH-128 insecure in practice. In other words, even if an attacker can extract the arbitrary modular square roots mod n, it is not clear for him/her how to apply this operation when only a short window of bits in the middle of the Rabin ciphertext is available [98]. The security of the SQUASH-128 method and its robustness against common attacks have been studied in more detail in [98]. More importantly, the SQUASH-128 can be implemented using approximately 1100 gates [98], which is almost one third of the gates required for Hummingbird (3220 gates) [101, 102, 103] and half of the gates required for GRAIN-128 (2133 gates) [104] and QUARK (2296 gates) [105], while GRAIN-128, Hummingbird and QUARK are three of the smallest hardware oriented cryptographic schemes.

3.4.3 The Proposed Protocol

In this section, we propose a new RFID protocol which solves the security problems mentioned in Section 3.2. This protocol is designed based on the challenge-response mechanism and uses the SQUASH-128 as the required one-way hash function. The principles of the proposed protocol is as follows: after the initialization phase, each tag contains its cur-

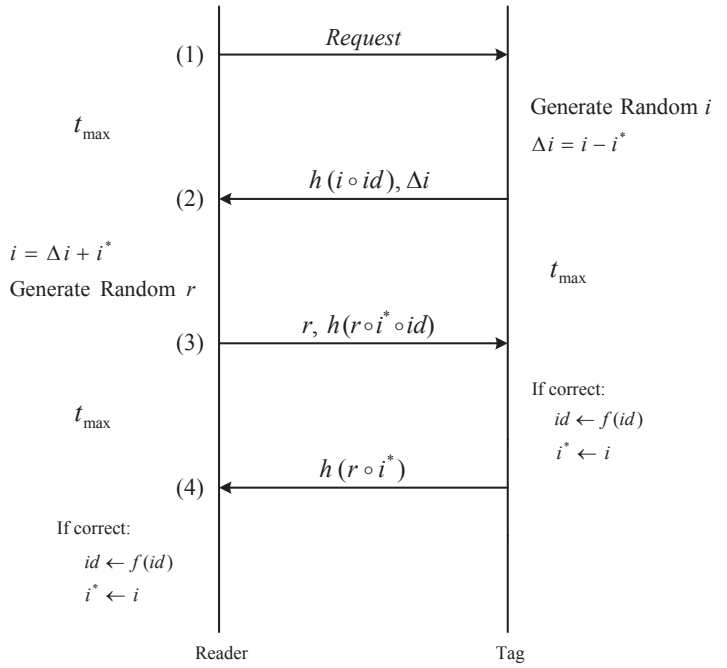

Figure 3.7: The proposed light-weight authentication protocol for RFID communications.

rent identifier id, the current session number i and the last successful session number i^*. Similarly, the database contains a list of all the identifiers and the last successful session numbers for all the tags in the system. In this scheme, both the database and the tags are aware of the hash function h. The communication process is shown in Fig. 3.7 and follows the steps below:

1. The reader sends a request message to the tag to start a new session. After sending the request message, the maximum time t_{max} that the reader waits for a valid reply by the tag is t. The reader resends the request message if a valid reply is not received in time t or if the received reply is not valid.

2. The tag generates a random integer number for i and calculates Δi by subtracting the last successful session number i^* from i. It also calculates $h(i \circ id)$ and sends it to the reader along with Δi. Here, $\circ$ is a suitable conjugation function as in Sections

3.2.2 and 3.2.3, and SQUASH-128 is used for h. The maximum time t_{max} that the tag waits for a valid reply by the reader is t.

3. The reader forwards the information received in step (2) to the database, where i is calculated using the received Δi and the stored i^*. The database checks all of the n entries and finds the tag whose id and i results in $h(i \circ id)$. It then generates a random challenge r, calculates $h(r \circ i^* \circ id)$, and sends the r and $h(r \circ i^* \circ id)$ to the tag via the reader. After sending the information in the third step, the reader waits at most for t seconds to receive a valid reply by the tag. The reader resends the request message if a valid reply is not received in time t or if the received reply is not valid.

4. The queried tag calculates $h(r \circ i^* \circ id)$ using the i^* and id it knows and the challenge r it has received from the reader, and compares it with the one sent by the reader. If they match, the tag changes its previous id using a function f which is known by both the tags and the database. It then calculates $h(r \circ i^*)$ and sends it to the reader as the acknowledgement of changing the old id.

5. After receiving the $h(r \circ i^*)$, the database calculates the tag's new id using the known function f and updates its list. It also updates the last successful session i^* with i as the final step.

We assume that the tags are close enough to the reader and they receive enough energy (from the reader) to back-scatter. We also assume that we have ideal communications environment, meaning that if the reader sends a message to a tag or a tag sends a message to the reader, the transmitted message is received correctly.

To provide the required security of the communication between the tags and the reader, our proposed protocol takes advantage of two main algorithms. Algorithm 3.1 is used by

Algorithm 3.1 The sequence of procedures used by the reader in the proposed light-weight authentication protocol.

1: Input id and i^* for all the tags in the system
2: Input n and t_{max}
3: Send a Request message
4: **for** time $= 0 : t_{max}$
5: Wait for $\{h(i \circ id), \Delta i\}$
6: **if** $\{h(i \circ id), \Delta i\}$ is received
7: **for** $j = 1 : n$
8: Calculate $i_j = \Delta i_j + i_j^*$
9: **if** $h(i_j \circ id_j) = h(i \circ id)$ (the received $\{h(i \circ id), \Delta i\}$ is correct)
10: Save j
11: Generate random r
12: Send r and $h(i \circ i_j^* \circ id_j)$ to the tag
13: **Break the loop** (go to line 19)
14: **end if**
15: **end for**
16: **end if**
17: **end for**
18: Go to line 3
19: **for** time $= 0 : t_{max}$
20: Wait for $\{h(r \circ i^*)\}$
21: **if** $\{h(r \circ i^*)\}$ is received
22: **if** $h(r \circ i_j^*) = h(r \circ i^*)$ (the received $\{h(r \circ i^*)\}$ is correct)
23: $id_j \leftarrow f(id_j)$
24: $i_j^* \leftarrow i_j$
25: Update the list
26: **Break the loop** (go to line 31)
27: **end if**
28: **end if**
29: **end for**
30: Go to line 3
31: Terminate the algorithm

the reader and Algorithm 3.2 is used by the tags. In Algorithm 3.1, n indicates the total number of tags present in the system, t_{max} shows the maximum waiting time, and index j refers to the tag whose i and id satisfy the criterion examined by the database.

Having explained our proposed protocol, we now consider the security threats mentioned in Section 3.2 and show the security improvements offered by the new protocol. We can mention the following improvements compared with the Henrici-Müller and Lim RFID protocols:

1. Unlike the challenge-response trigger protocol, it is not possible for an attacker to

Algorithm 3.2 The sequence of procedures used by the tags in the proposed light-weight authentication protocol.

```
1:  Wait for the Request message
2:  if the Request message is received
3:    Generate a random i
4:    Calculate Δi = i − i*
5:    Send {h(i ∘ id), Δi} to the reader
6:  end if
7:  for time = 0 : t_max
8:    Wait for a message
9:    if the Request message is received
10:     Break the loop (go to line 3)
11:   else if the {r, h(r ∘ i*_j ∘ id_j)} message is received
12:     if h(r ∘ i*_j ∘ id_j) = h(r ∘ i* ∘ id)    (the received {r, h(r ∘ i*_j ∘ id_j)} is correct)
13:       id ← f(id)
14:       Send h(r ∘ i*) to the reader
15:       i* ← i
16:       Break the loop (go to line 21)
17:     end if
18:   end if
19: end for
20: Go to line 3
21: Terminate the algorithm
```

make a dictionary of the inputs and use it to interrogate the tags, impersonate them as the legitimate tags or to track an interrogated tag. The reason is that the reader does not use any challenge in step (1) of Fig. 3.7, and the response of the tag in step (2) is changed dynamically over time because of the random nature of i which makes it impossible for the attackers to track a static $h(i \circ id)$.

2. Unlike the Henrici-Müller protocol, the value of i does not increase over time but changes randomly (it may increase or decrease) for each request message. Therefore, it is not possible for an attacker to abnormally increase the value of Δi and track the target tag using this large value.

3. Unlike the Henrici-Müller and the challenge-response trigger protocols, it is not possible to track a tag based on the static information it sends. The reason is that i changes randomly after each request message in step (1), therefore, each time the

$h(i \circ id)$ and Δi are different from the previous time (after each interrogation).

4. Unlike the Henrici-Müller, the challenge-response trigger and the forward rolling schemes, it is not possible for an attacker to corrupt the synchronization between the interrogated tag and the reader after step (1) and before step (3). The reason is that in the third step, the reply from the reader depends on i^*, not i nor the challenge sent from the tag to the reader in step (2). For example, assume that the legitimate reader sends a request message to a tag and receives $\Delta i_1 = i_1 - i^*$, but before step (3), an attacker sends another request message to the tag as well. In this case, $\Delta i_2 = i_2 - i^*$ is generated and sent by the tag but i^* and id are not changed. The legitimate reader finds the interrogated tag in its database list using $h(i_1 \circ id)$ and replies with r and $h(r \circ i^* \circ id)$. The response does not depend on i_1 or i_2 but only depends on i^*. On the other hand, the attacker cannot send the correct $h(r \circ i^* \circ id)$ as it does not have access to i^*. Therefore, the synchronization between the tag and the reader is not affected by this attack. From another point of view, the attacker cannot de-synchronize the reader and the tag by sending a fake pattern of the $\{h(i \circ id), \Delta i\}$ to the reader in the second step. This is because of considering the t_{max} in the algorithm. After sending the request message in the first step, the reader waits for a maximum of t_{max} to receive a valid reply from the tag. If the reader receives a valid $\{h(i \circ id), \Delta i\}$, it simply goes to the third step and sends back the $\{r, h(r \circ i^* \circ id)\}$. However, if an attacker sends an invalid $\{h(i \circ id), \Delta i\}$ before the legitimate tag replies, the reader checks the received information and after finding that the received $\{h(i \circ id), \Delta i\}$ is invalid, it still waits for t_{max} seconds and gives the legitimate tag the chance to send its valid $\{h(i \circ id), \Delta i\}$ (Algorithm 3.1 line 4). The same mechanism is used to guarantee that the attacker cannot de-synchronize the reader and the tag by sending a fake $\{r, h(r \circ i^* \circ id)\}$ to the tag in the third step

(Algorithm 3.2 line 7) or by sending a fake $h(r \circ i^*)$ to the reader in the fourth step (Algorithm 3.1 line 19).

5. Unlike the forward rolling trigger scheme, the number of sessions between the tag and the reader is not limited in the proposed protocol because this protocol only uses a simple one-way hash function and does not rely on Lamport's authentication method [99].

6. Unlike the Henrici-Müller scheme, the attacker cannot use the null element for the challenge r in step (3) of the proposed protocol because the attacker cannot obtain the value of $h(i^* \circ id)$ from $h(i \circ id)$ in step (2).

7. The proposed method is robust against the replay attack. An attacker can capture a tag and interrogate it, but it can only obtain $h(i \circ id)$ and Δi. The attacker can use this information to reply to a request message from the legitimate reader in step (2) of the proposed protocol, but it cannot impersonate itself to the reader as the reader waits for the $h(r \circ i^*)$ response from the attacker in step (4). On the other hand, the attacker cannot obtain any knowledge about i^* by interrogating a captured tag. The attacker cannot send the correct $h(r \circ i^*)$ to the reader and the reader does not update the identification of the tag in the database list. Therefore, the replay attack cannot affect the proposed protocol.

8. In the proposed protocol, only the most recent and updated id is kept and the previous id is deleted from the database list after receiving the $h(r \circ i^*)$ message in step (4). Therefore, attackers cannot eavesdrop on the communication between a legitimate reader and a real tag to use it for misleading the reader. After each successful session, the id is updated and therefore, the information in step (2) of Fig. 3.7 will not be accepted anymore by the database.

Table 3.1: Security comparison of the proposed protocol and the light-weight authentication schemes explained in Section 3.2.

Protocol\Attack	Tracking	De-synchronization	Replay	DoS	Impersonation
Standard Gen-2 [4]	No	No	No	Yes	No
Henrici-Müller [5]	No	No	No	Yes	No
Challenge-Response Trigger [6]	No	No	Yes	Yes	No
Forward Rolling Trigger [6]	No	No	Yes	No	No
Server-less Method [7]	No	No	Yes	Yes	No
Gen-2$^+$ [4]	No	No	No	Yes	No
Proposed method	Yes	Yes	Yes	Yes	Yes

In this chapter, we aimed to propose a new RFID protocol which solves the security and privacy issues of the protocols introduced in [3, 4, 5, 6, 7], and to improve the reliability of the reader-tag communication in the RFID systems. We simply showed that unlike the previously discussed schemes, our proposed protocol is not vulnerable to tracking, de-synchronization, replay, DoS and Impersonation attacks. Formal cryptographic analysis of the schemes introduced in [3, 4, 5, 6, 7] and the proposed protocol is beyond the scope of this chapter, however, there exist many cryptographic frameworks that can be used to evaluate these protocols [107, 108, 109, 110].

3.5 Summary

In this section, we compare the security aspects of the proposed protocol with the standard Gen-2 method [3] and the five light-weight authentication schemes [4, 5, 6, 7] explained in Section 3.2. Besides the security aspects, the complexity and computational costs are compared. We show that the proposed protocol does not impose too much computational demand on the RFID tag while significantly improving the security of RFID systems. Table 3.1 compares our proposed protocol with the schemes discussed in Section 3.2, and confirms the robustness of the proposed protocol against the studied attacks. In this table, tracking, de-synchronization, replay, DoS, and impersonation are considered as common

Table 3.2: Complexity comparison of the proposed protocol and the light-weight authentication schemes explained in Section 3.2.

Protocol	**Complexity**
Standard Gen-2 [3]	2β
Henrici-Müller [5]	$4\alpha+2\lambda$
Challenge-Response Trigger [6]	$3\alpha+\beta+2\lambda$
Forward Rolling Trigger [6]	$4\alpha+\beta$
Server-less Method [7]	$3\alpha+\beta+4\lambda$
Gen-2^+ [4]	$2\beta+\lambda+\theta$
Proposed method	$4\alpha+\beta+3\lambda$

RFID threats that may affect the light-weight authentication protocols. These attacks are defined in Section 3.2. For each attack, the word "Yes" shows that the considered protocol is robust against that attack while "No" means that the protocol is vulnerable to that attack. As can be inferred from Table 3.1, the standard Gen-2 [3], Henrici-Müller [5], challenge-response trigger [6], forward rolling trigger [6], server-less method [7], and Gen-2^+ [4] protocols are all vulnerable to the tracking, de-synchronization, and impersonation attacks. The challenge-response trigger, forward rolling trigger and server-less schemes, however, can resist the replay attack, and DoS is a problem only for the forward rolling trigger protocol. On the other hand, the proposed method can provide robustness against tracking, de-synchronization, replay, DoS, and impersonation attacks.

As explained before, the more computationally demanding a protocol is, the less attractive it is for real RFID applications. Therefore, the complexity and computational demand of the protocol should be considered as an important factor when designing an RFID communication scheme. The main bottleneck in designing RFID protocols is the limitation in the computational ability of the tags and not the readers, as the readers can take advantage of advanced processors. In this study, we only consider the computations performed by the tags and neglect the computational costs of the reader. Table 3.2 compares the computational costs for each of the six RFID schemes, as well as our proposed protocol. In order to make a fair comparison of the complexity and computational costs,

we denote the computational cost of each hash function by α, each random generation by β, each conjugation or concatenation function by λ, and each Hamming distance calculation by θ. No matter which hash function is used, it would be a plausible assumption that α has the most impact on the total computational costs among α, β, λ and θ. As an example, it can be shown that each round of calculating α using the Hummingbird scheme needs 8 modulo 2^{16} addition, 80 XOR and 80 S-box calculation. As another example, each round of calculating α using the SQUASH-128 scheme needs one modulo $2^{128} - 1$ addition.

It should be noted that among all the compared schemes, the proposed protocol is the only one that takes advantage of the SQUASH-128 method. As a result, it imposes the lowest computational cost on the tags for hash calculation. In order to have a completely fair comparison, however, we consider the case where all the discussed protocols are assumed to have used the SQUASH-128 method. This way, we assume that for each hash calculation, all the compared protocols have the same computational cost of α. As can be inferred from Table 3.2, the standard Gen-2 protocol has the lowest computation demands. Except for the Gen-2 and Gen-2^+ schemes, the other protocols need at least three hash computations and the only scheme that needs an extra circuitry for calculating the Hamming distance of two binary strings is Gen-2^+. Finally, all the protocols except the standard Gen-2 and the forward rolling trigger need to perform at least one conjugation or concatenation. It can be inferred from Table 3.2 that the proposed protocol does not impose a significant amount of computational costs on the tags. Having an extra simple circuitry (to calculate a hash function or a Hamming distance) seems to be a plausible and necessary assumption for increasing the security of communication between the tags and the readers, as discussed in [4, 5, 6, 7, 19, 22, 97]. Among the six schemes discussed in Sections 3.2.1 to 3.2.5 and the one we proposed in Section 3.4.3, only the server-less protocol proposed by Tan *et al.* [7] does not depend on the direct access to a central database. Finally, it should be noted

that except for the new proposed protocol, all the discussed protocols are vulnerable to tracking, de-synchronization and impersonation attacks.

In the proposed light-weight authentication protocol, we take advantage of the SQUASH-128 hash function. The main reasons that we choose SQUASH-128 are ease of implementation (in terms of the number of required gates), suitability for RFID applications and difficulty of breaking SQUASH-128. However, it should be noted that any other efficient hash function can be used in the proposed authentication protocol. The use of SQUASH-128 can also be beneficial to other studied protocols which use hash functions.

We do not claim that the proposed protocol can resist all possible attacks and security threats, however, it was shown that the proposed protocol improves the security of communication between the readers and the tags in RFID systems, and solves many security issues of the schemes proposed in [3, 4, 5, 6, 7].

Chapter 4

Probabilistic Tag Estimation Method

4.1 Introduction

An RFID system consists of one (or more) reader(s) and a certain number of tags. The reader communicates with the tags to retrieved their data. Due to the shared nature of the communication channel, packet collisions occur when multiple tags simultaneously transmit their data to the reader. Therefore, an efficient anti-collision protocol is of great importance to save the bandwidth and energy needed and to reduce the identification delays in RFID systems. Many anti-collision protocols have been proposed to solve the collision problem in RFID systems. These protocols can be generalized into two main groups; the tree-based protocols and the ALOHA-based protocols. The tree-based protocols divide a set of tags into two subsets in each step until there is only one tag left. In ALOHA-based protocols, the tags transmit their data at random during the time frames previously assigned to all tags by the reader. The ALOHA technique has a series of variants such as pure ALOHA (PA), framed slotted ALOHA (FSA) and dynamic framed slotted ALOHA (DFSA). Among them, the DFSA technique is the most efficient one since it adjusts the frame size prior to each query [111]. For DFSA-based protocols, it has been shown that the maximum throughput is achieved when the frame size is equal to the number of tags in the system [2, 93, 111, 112]. Therefore, we need to have an accurate tag estimate method to be able to design more efficient DFSA-based protocols. Estimating the number of RFID tags (and accordingly the number of objects) in an area of interest is also one

of the primary tasks in many applications, such as counting the number of conference or exhibition attendees with RFID badges [93], verifying the number of products with RFID labels in cargo shipping at the airport [113], etc. The problem of estimating the number of RFID tags can be easily reduced to identifying the IDs of all RFID tags and counting them. As mentioned before, there are a number of schemes proposed for solving the tag identification problem and they can be directly borrowed to compute the exact number of RFID tags when the size of the RFID system is small. Those solutions, however, become infeasible when the RFID system scales up [114].

It is not always necessary to know or count the exact number of tags in an RFID system. For many application scenarios, knowing the approximate number of tags in the system is adequate. Moreover, since each tag ID is linked to a specific object or person, it is not always allowed to use the tag IDs directly for counting the number of tags for security and privacy reasons. For instance, the attendees of an exhibition may not wish to reveal which of the service providers they were interested in when visiting the exhibition, or the attendees of a conference may not like to reveal the name of the sessions they attended during their visit [10]. Therefore, in many cases we need some alternative approaches to estimate the number of tags in an area of interest without directly reading all the tag IDs. In accordance with this need, a set of probabilistic counting schemes have been proposed to estimate the approximate number of tags in the RFID systems [2, 10, 72, 93, 115, 116].

In [2], Chen proposed a novel tag estimation algorithm for the ALOHA-based anticollision protocols. In this approach, the reader estimates the number of remaining tags in the RFID system after each interrogation based on *a posteriori* probability and uses this estimated number to determine the number of required time slots for the next interrogation. This approach can improve the performance of the ALOHA-based RFID anticollision algorithms. However, there exists an error in the probabilistic modeling of the problem.

In this chapter, we take advantage of the probabilistic model we developed in Chapter 2 and correct the tag estimation method proposed by Chen [2]. Briefly, the contributions of this chapter are as follows:

- We first show that the probabilistic model proposed in [2] is incorrect. We then present the correct probabilistic model.
- Our proposed model is validated via simulation. We also compare the simulation results with the model suggested in [2] and our proposed model. The results from our probabilistic model closely match with the simulation results.
- The consequences of using the model suggested in [2] are shown and the required corrections are identified.

The rest of this chapter is organized as follows: Section 4.2 summarizes the probabilistic model proposed in [2] and discusses its problem. The correct probabilistic model for the ALOHA-based RFID systems is presented in Section 4.3. Some validating simulation results and the corrections required for the probabilistic model proposed in [2] is provided in Section 4.4, followed by the summary in Section 4.5.

4.2 Probabilistic Model Proposed by Chen

In this section, we summarize the probabilistic model proposed in [2]. In ALOHA-based RFID systems, the time frame is divided into time slots. Each tag chooses one of these time slots randomly and transmits its ID in the reply message. In each time slot, three events may happen. If only one tag chooses a specific time slot and transmits its ID, then the transmission is successful. This time slot is called a *single* time slot. If more than one tag selects a specific time slot, then a packet collision will occur and the reader will not

be able to decode the received signal. This is called a collided time slot. Finally, if no tag chooses a specific time slot, the reader will observe an empty time slot. If the reader chooses the number of slots in a frame to be much higher than the number of tags, then the channel capacity is wasted and the reader will observe multiple empty time slots. On the other hand, if the reader chooses the frame size to be much smaller than the number of tags, then the chance of collision will increase. It has been proved that for optimal performance, the number of time slots in a frame is equal to the number of tags in the system [2, 93, 111, 112].

A probabilistic model for ALOHA-based RFID systems was proposed in [2]. In that model, the reader first selects a predefined number of time slots (128) to be the frame size. It then transmits a query message. Each tag randomly chooses a time slot and sends its reply in that time slot. After the first interrogation, the reader estimates the number of tags $\hat{n}$ in the system, based on the *maximum a posteriori probability* obtained from the number of empty (E), single (S) and collided (C) time slots. Then, the reader selects the frame size to be equal to $(\hat{n} - S)$ and proceeds with the next interrogation. At the end of each interrogation, the values of $\hat{n}$, E, S and C are being updated. This procedure continues until all the tags are identified in the system. In each interrogation, the summation of E, S and C is equal to L, which is the total number of time slots in the frame.

In [2], Chen suggested to first calculate the probability of observing E empty, S single and C collided time slots, $P(E, S, C)$, and then find the $\hat{n}$ which maximizes this probability for each interrogation. He mentioned that in an RFID system containing n tags, the number of tags allocated in a time slot is a binomial distribution with n Bernoulli experiments and $\frac{1}{L}$ as the occupied probability. The probability of finding r tags in a time slot is given by [2]

$$B(r) = \binom{n}{r} \left(\frac{1}{L}\right)^r \left(1 - \frac{1}{L}\right)^{n-r} \quad , \quad 0 \leq r \leq n \ . \tag{4.1}$$

The probability of observing an empty slot, a single slot, and a collided slot can be obtained respectively as [2]

$$p_e = B(0) = \left(1 - \frac{1}{L}\right)^n, \tag{4.2}$$

$$p_s = B(1) = \frac{n}{L}\left(1 - \frac{1}{L}\right)^{n-1}, \tag{4.3}$$

$$p_c = 1 - p_e - p_s. \tag{4.4}$$

In the next step, the probability of observing E empty, S single and C collided time slots, $P(E, S, C)$, was derived. In [2], the the problem was modeled as a multinomial distribution with L repeated *independent* trials (choosing a time slot by a tag), where each trial can result in an empty, single or collision event. However, *these events are not independent*, that is, the probability of observing E empty time slots affects the probability of observing S single time slots, and these two probabilities affect the probability of observing C collisions. Based on the wrong assumption mentioned, $P(E, S, C)$ was calculated in [2] as

$$\begin{aligned} P(E,S,C) =& \frac{L!}{E!S!C!}\left[\left(1-\frac{1}{L}\right)^n\right]^E\left[\frac{n}{L}\left(1-\frac{1}{L}\right)^{n-1}\right]^S \\ & \times\left[1-\left(1-\frac{1}{L}\right)^n-\frac{n}{L}\left(1-\frac{1}{L}\right)^{n-1}\right]^C. \end{aligned} \tag{4.5}$$

After finding $P(E, S, C)$, Chen's algorithm finds $\hat{n}$ which maximizes $P(E, S, C)$. That is $\hat{n} = \arg\max_n P(E, S, C)$. This $\hat{n}$ is considered as the estimation of n, which is the number of tags remained in the system. The algorithm proposed in [2] is shown in Algorithm 4.1.

Although the approach proposed in [2] is rational, the results are inaccurate due to the mentioned mistake in calculating $P(E, S, C)$. Based on the above, a correct probabilistic

Algorithm 4.1 The anticollision algorithm used in [2]

1: $L := 128$
2: Initialize E, S and C ($C \neq 0$)
3: $counter := 0$
4: **while** $C \neq 0$
5: Interrogate all tags
6: $counter := counter + 1$
7: update E, S and C
8: $\hat{n} := \arg\max_n P(E, S, C)$
9: $L := \hat{n} - S$
10: **end while**

model for ALOHA-based RFID systems is needed. By using the correct model and the approach proposed in [2], the reader would be able to estimate the number of tags in the system accurately and assign an appropriate number of time slots in the frame for the next interrogation.

4.3 Correct Probabilistic Model of the ALOHA Systems

As explained in Section 4.2, the formulation proposed in [2] is incorrect because it is assumed that the events of observing empty, single and collided time slots are independent from each other. This assumption is not valid and the mentioned events are dependent on each other. In this section, we take advantage of the probabilistic model we developed in Chapter 2 and present the correct derivation of the probability $P(E, S, C)$.

We need to model our system mathematically and find the probability of observing a specific frame structure (E empty, S single and C collided time slots). We consider a frame structure which has E empty slots in its first section, S single slots in the second section, and C collided slots in the last section, as it is depicted in Fig. 4.1. In this figure, each small circle in a time slot represents a single tag which has sent its ID in that time slot. Therefore, empty time slots are shown without any circle, single time slots are shown with

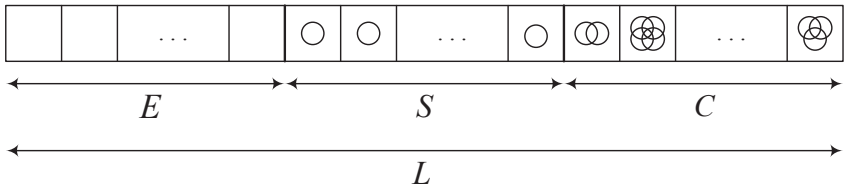

Figure 4.1: The empty, single and collided sections of a time frame in the analytical model.

one circle, and collided time slots are shown with multiple circles inside them.

In the model, the frame length is equal to L, while n represents the number of remaining RFID tags in the system. First, the probability of observing E empty slots in the first part of the frame is considered. This probability is denoted by $P_1(E)$ and is equal to

$$P_1(E) = \left(1 - \frac{E}{L}\right)^n, \qquad 0 \leq E \leq L \ . \tag{4.6}$$

In the next step, the probability of observing S single time slots in the second part of the frame conditioned to observing E empty slots in the previous step is considered. This probability is denoted by $P_2(S \mid E)$

$$\begin{aligned} P_2(S \mid E) = & \binom{n}{S} \left(\frac{S}{L-E}\right)^S \left(1 - \frac{S}{L-E}\right)^{(n-S)} \\ & \times \left(\sum_{i=0}^{S} (-1)^i \binom{S}{i} \left(1 - \frac{i}{S}\right)^S\right), \\ & 0 \leq S \leq \min\{L-E, n\} \end{aligned} \tag{4.7}$$

where $\left(\frac{S}{L-E}\right)^S$ is the probability that S tags are assigned to the first S slots among the total remaining $(L-E)$ slots, $\left(1 - \frac{S}{L-E}\right)^{(n-S)}$ shows the probability that the remaining $(n-S)$ tags are assigned to the remaining $(L-E-S)$ slots, and finally the summation $\sum_{i=0}^{S} (-1)^i \binom{S}{i} \left(1 - \frac{i}{S}\right)^S$ is the probability that the mentioned S tags are assigned to S slots,

with no basket empty, or in other words, each of the S slots only accommodates one and only one of the S tags (same as the classical urn model). The summation $\sum_{i=0}^{S}(-1)^i\binom{S}{i}\left(1-\frac{i}{S}\right)^S$ can be simplified as

$$\sum_{i=0}^{S}(-1)^i\binom{S}{i}\left(1-\frac{i}{S}\right)^S=\frac{S!}{S^S}\ . \tag{4.8}$$

Based on the above, $P_2(S \mid E)$ can be written as

$$\begin{aligned} P_2(S \mid E) &= \binom{n}{S}\left(\frac{S}{L-E}\right)^S\left(1-\frac{S}{L-E}\right)^{(n-S)}\frac{S!}{S^S} \\ &= \binom{n}{S}\left(\frac{(L-E-S)^{(n-S)}}{(L-E)^n}\right)S!\ . \end{aligned} \tag{4.9}$$

Now, we need to calculate the probability of observing C collisions in the last section of the frame conditioned to observing E empty and S single time slots in the previous steps. For $P_3(C \mid E, S)$, it is not that simple to calculate the probability of observing C collisions conditioned to E and S directly. Therefore, we define a class of acceptable events which represents different ways of distributing $(n-S)$ tags in C slots such that each slot contains *at least* two tags. By defining the number of these acceptable events as $g_{n-S}(C,2)$, we have

$$P_3(C \mid E, S)=\frac{g_{n-S}(C,2)}{C^{(n-S)}}\ , \tag{4.10}$$

in which $C^{(n-S)}$ is the total number of ways that we can assign $(n-S)$ tags to the remaining C time slots. Now, the main problem is to determine $g_{n-S}(C,2)$. Riordan [96] suggested two closed form expressions for $g_\alpha(m,s)$ using the classical urn model in which α, m and s denote the number of balls, the number of urns, and the minimum number of balls in each urn, respectively. The first closed form expression for $g_\alpha(m,s)$ is

$$g_\alpha(m,s)=mg_{\alpha-1}(m,s)+m\binom{\alpha-1}{s-1}g_{\alpha-s}(m-1,s), \tag{4.11}$$

and the second one is

$$g_\alpha(m,s) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} \frac{\alpha!}{(s-1)!^k(\alpha - sk + k)!} \times g_{\alpha - sk + k}(m-k, s-1). \tag{4.12}$$

Using Eq. (4.11) and (4.12), we can find the exact number of acceptable events in Eq. (4.10) by replacing α with $(n - S)$, m with C and s with 2 for our problem. The above recursive equations can be calculated in two different ways. In the first approach, we can only use Eq. (4.11) and combine it with three simple logical constraints, as stated below:

a) **if** $(\alpha \neq 0)$ **and** $(m = 0)$, **then** $g_\alpha(m, s) = 0$;

b) **if** $(\alpha < ms)$, **then** $g_\alpha(m, s) = 0$;

c) **if** $(m = 1)$ **and** $(\alpha \neq 0)$ **and** $(\alpha \geq ms)$, **then** $g_\alpha(m, s) = 1$.

Using this method, we can start from an initial point and find the exact value for $g_\alpha(m, s)$ recursively. As the second approach, we can simplify Eq. (4.12) by replacing s with 2 and write

$$g_\alpha(m,2) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} \frac{\alpha!}{(\alpha - k)!} g_{\alpha-k}(m-k, 1) \tag{4.13}$$

in which

$$g_{\alpha-k}(m-k,1) = p_0(\alpha - k, m - k)\ (m-k)^{(\alpha-k)}\ , \tag{4.14}$$

and $p_0(\alpha - k, m - k)$ is the probability that we have $(\alpha - k)$ tags and $(m - k)$ time slots and all the slots contain at least one tag. From [95], we have the mathematical expression for $p_0(\alpha - k, m - k)$ as

$$p_0(\alpha - k, m - k) = \sum_{v=0}^{m-k} (-1)^v \binom{m-k}{v} \left(1 - \frac{v}{m-k}\right)^{(\alpha-k)} . \tag{4.15}$$

By substituting Eq. (4.14) and (4.15) into Eq. (4.13), we have

$$\begin{aligned} g_\alpha(m,2) = & \sum_{k=0}^{m} \sum_{v=0}^{m-k} (-1)^{(k+v)} \binom{m}{k} \binom{m-k}{v} \\ & \times \frac{\alpha!}{(\alpha-k)!} (m-k-v)^{(\alpha-k)} \ . \end{aligned} \tag{4.16}$$

Based on the above, Eq. (4.10) can be written as

$$\begin{aligned} P_3(C \mid E,S) = & \sum_{k=0}^{C} \sum_{v=0}^{C-k} (-1)^{(k+v)} \binom{C}{k} \binom{C-k}{v} \\ & \times \frac{(n-S)!}{(n-S-k)!} \frac{(C-k-v)^{(n-S-k)}}{C^{(n-S)}} \ . \end{aligned} \tag{4.17}$$

Using Eq. (4.6), (4.9), (4.10) and (4.16) or (4.11), we can determine $P(E,S,C)$, which is the probability of observing E empty, S single and C collided slots as

$$P(E,S,C) = \left(\frac{L!}{E!\ S!\ C!} \right)\ P_1(E)\ P_2(S \mid E)\ P_3(C \mid E,S) \ . \tag{4.18}$$

In Eq. (4.18), $\left(\frac{L!}{E!\ S!\ C!}\right)$ is the number of ways that the three mentioned sections in Fig. 4.1 can be scrambled and mixed with each other and make a random structure of E empty, S single and C collided time slots. As it can be observed from Eq. (4.18), the probability $P(E,S,C)$ is a product of three other probabilities which are related to each other. The correct formula for calculating $P(E,S,C)$ is Eq. (4.18), which is different from Eq. (4.5).

4.4 Performance Evaluation

In this section, we show that Eq. (4.5) is not confirmed by simulations while Eq. (4.18) agrees with the simulation results. Based on the new formulation, some of the figures in [2] need to be changed. These corrections are also provided in this section.

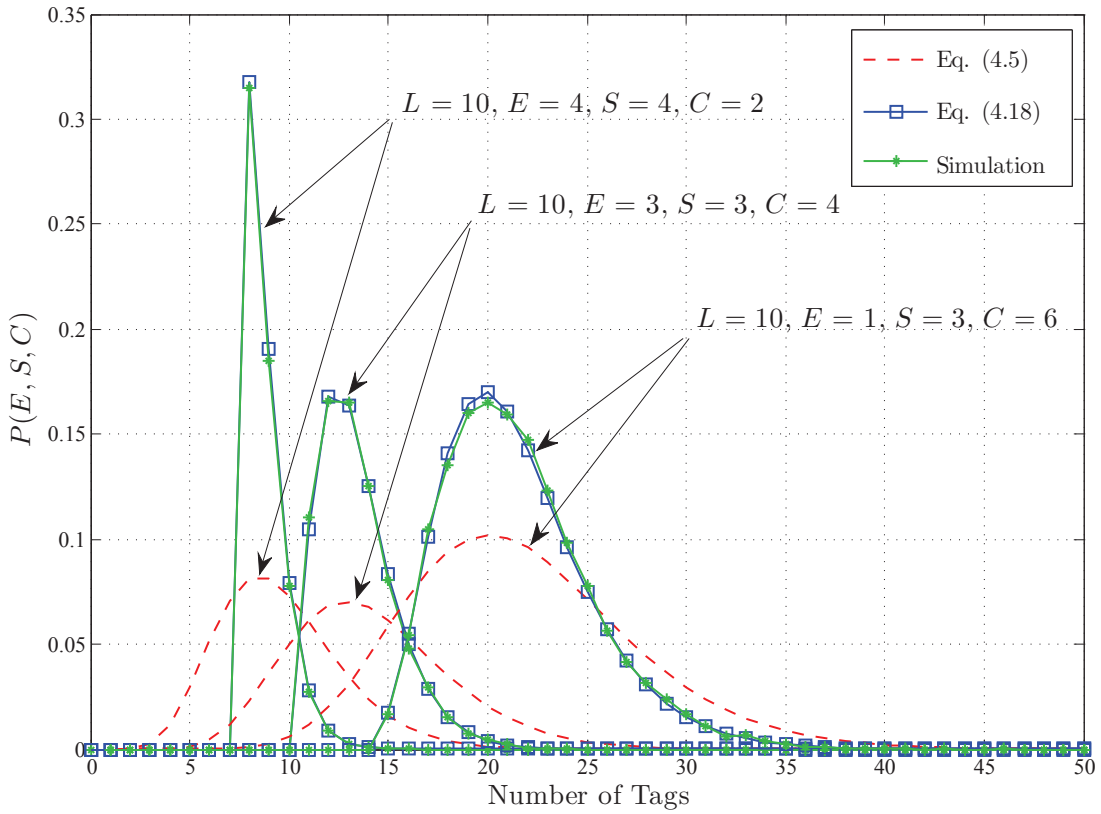

Figure 4.2: *A posteriori* probability distributions using Eq. (4.5) from [2], Eq. (4.18), and the actual probabilities for a simulated RFID system.

Fig. 4.2 shows the probability $P(E, S, C)$ obtained using Eq. (4.5) which was proposed in [2], the correct formula shown in Eq. (4.18), and the actual probability obtained via simulation. For the simulation, we used MATLAB and obtained the probability $P(E, S, C)$, using 10,000 iterations. The probabilities are plotted for three cases, ($L = 10$, $E = 4$, $S = 4$, $C = 2$), ($L = 10$, $E = 3$, $S = 3$, $C = 4$) and ($L = 10$, $E = 1$, $S = 3$, $C = 6$). The probabilities obtained via simulation are then compared with the probabilities obtained from Eq. (4.5) as well as the probabilities obtained from Eq. (4.18). As it can be inferred from Fig. 4.2, Eq. (4.5) does not match with the results obtained from simulating an RFID system. The peaks obtained from Eq. (4.5) are lower than the simulated system and at some points, these peaks occur with one unit shift to the right on n axis comparing to the

simulated system. On the other hand, the probabilities obtained from Eq. (4.18) match with the simulated system. The peaks of $P(E, S, C)$ happen with the same heights and without any shift comparing to the simulated system.

We can also conclude that Eq. (4.5) is incorrect from Fig. 4.2 without relying on the simulated RFID system. If we observe $P(E, S, C)$ plotted for ($L = 10$, $E = 4$, $S = 4$, $C = 2$) and obtained from Eq. (4.5) at point $n = 5$, we can notice a positive value which is logically impossible. This probability should be equal to 0 because it is not possible to observe $E = 4$, $S = 4$, $C = 2$ while we have only $n = 5$ tags in the system. Logically, $P(E, S, C)$ should be equal to 0 for values of n less than 8.

As another correction, a table was presented in [2] which showed the estimated number of tags for an RFID system (TABLE I in [2]). In this table, the number of tags were estimated based on *a posteriori* probability scheme for different values of S and C. We checked the values obtained from Eq. (4.18) with the values obtained from Eq. (4.5). Although the heights of the peaks for Eq. (4.18) and (4.5) are different, the values of n where the peaks happen are the same in some cases. However, in some other cases, the values of n where the peaks happen are different for Eq. (4.18) and (4.5). The correct values of estimated n are presented in Table 4.1. The numbers shown in bold red color

Table 4.1: Correct values of the estimated n (number of tags) for the algorithm in [2] ($L = 10$)

		C									
		0	1	2	3	4	5	6	7	8	9
S	1	**2**	3	4	5	6	7	8	9	10	11
	2	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	-
	3	**6**	**7**	**8**	**9**	11	12	13	14	-	-
	4	**9**	**10**	**11**	**12**	14	15	16	-	-	-
	5	12	**13**	**14**	16	17	19	-	-	-	-
	6	**15**	17	**18**	20	**21**	-	-	-	-	-
	7	20	**21**	23	25	-	-	-	-	-	-
	8	26	28	30	-	-	-	-	-	-	-
	9	35	38	-	-	-	-	-	-	-	-
	10	**50**	-	-	-	-	-	-	-	-	-

(bold gray color in black and white print) are different from those calculated by Chen in [2] while the numbers in black color are the same for both Eq. (4.5) and (4.18) and therefore, they are the same as the values shown in [2].

4.5 Summary

In this chapter, we showed that the tag estimation proposed by Chen [2] is incorrect. Using the probabilistic model we developed for ALOHA-based RFID systems in Chapter 2, we corrected the probabilistic tag estimation method proposed in [2]. The modified probabilistic model was verified via simulations and compared with the one proposed in [2]. Simulation results confirmed that our modified probabilistic tag estimation method completely matches the results of real ALOHA-based RFID systems.

An ideal ALOHA-based RFID system has been modeled in [2] and modified in this chapter, however, there exist some other technical aspects that can be targeted for future works and further contributions. For instance, in our modified probabilistic tag estimation method and the one proposed in [2], it has been assumed that the length of the E, S and C time slots are all equal in ALOHA-based RFID systems, while the length of these slots might be different in some specific types of ALOHA-based RFID protocols [90]. As another example, it has been assumed that the reader does not make any mistake in deciding whether a time slot is singly occupied or collided. However, this may not be always true because of some technical issues. Some of the time slots which are interpreted as singly occupied can actually be collided slots [117, 118]. Moreover, it has been assumed that if a tag transmits its data in a single slot, the reader will receive this data for sure. In other words, the probability of transmission error has been considered to be zero in the ideal studied model. However, this may not be always true considering the noise and the interference in wireless channels [118]. Finally, in the modified probabilistic tag estimation

method and in [2], it has been assumed that the length of the frame (L) can be any integer from 1 to 128, however, many protocols have specific constraints on the length of the frame. For instance, the length of the frame in EPC Class-1 Gen-2 standard should be an integer of the form $L = 2^Q$, where Q is an integer value between 0 and 15 [1, 3]. Finally, the field nulls effect and its role in losing the power of tags is another technical issue which can be considered in a non-ideal ALOHA-based RFID system [119].

The modified tag estimation method relies on estimating the number of tags that maximizes the probability of observing a combination of empty, single and collided slots by the reader. Although this estimation adds some computational costs to the system, it is performed in the reader (or database). Therefore, using the proposed method does not impose any additional computation on the tags.

Chapter 5

Analytical Modeling and Performance Analysis of the EPCglobal Class-1 Generation-2 Protocol

5.1 Introduction

An RFID reader is able to communicate with a single tag at a time, yet RFID systems are prone to transmission collisions due to the shared nature of the wireless channel used by tags. In order to solve the collision problem, the tree-walking and the ALOHA-based anti-collision protocols have been proposed [20, 53, 55, 57, 58, 59]. Recently, a framed-slotted ALOHA-based anti-collision scheme has been standardized by EPCglobal [3]. This scheme is called the EPC Class-1 Generation-2 (briefly EPC Gen-2) protocol. The EPC Gen-2 has been accepted as the main standard protocol for inventory checking, supply chain management and many other applications. Most RFID consumers currently use the EPC Gen-2 protocol [1]. Although the EPC Gen-2 protocol has been used as the main standard for supply chain management applications, there are only a few works that have studied the performance of this protocol from the quantitative point of view [1, 68, 120].

To address this issue, Wang *et al.* studied the performance of the EPC Gen-2 protocol and modeled it as a Markov chain system [1]. This Markov chain interpretation of the EPC Gen-2 protocol offers a useful way for studying this protocol and helps researchers to better understand and improve it. Although this Markov chain model is useful in obtaining a quantitative performance analysis of the EPC Gen-2 protocol, it does not provide an explicit analytical framework for the EPC Gen-2 protocol. In other words, we need to run simulations and average the obtained results if we use the model suggested in [1] for studying the behavior of the EPC Gen-2 protocol. Moreover, the accuracy of this model decreases as the number of tags in the system increases. To solve the accuracy issue, we modify the model proposed in [1] and propose a new Markov chain model for the EPC Gen-2 protocol. More importantly, we "formulate" our proposed Markov chain model. Using our new model and the formulae derived, we are able to directly calculate how many queries are needed and how many bits are transmitted to identify all tags in a system that uses the EPC Gen-2 protocol, without needing any simulations. Such a performance analysis is helpful for RFID system deployment and in designing new algorithms to improve the tag identification performance. Moreover, this chapter provides an analytical model for researchers in the field to easily compare their proposed protocols with the standard EPC Gen-2 protocol. Simulation results confirm that our Markov model accurately represents the EPC Gen-2 protocol and is more accurate than the model proposed in [1]. The proposed analytical model outperforms the Markov model in [1] for two reasons. First, the model proposed in [1] uses an approximation of the EPC Gen-2 protocol while our analytical model takes advantage of the exact interpretation of the EPC Gen-2 protocol. Second, unlike the analytical model in [1] which relies on simulations, our proposed model uses accurate and closed form analytical formulae for calculating the expected number of queries and the expected number of transmitted bits in an RFID system.

The contributions of this chapter are as follows:

1. We study the EPC Gen-2 protocol and the Markov model proposed for it in [1]. Then we modify this model and propose a more accurate Markov model for the EPC Gen-2 protocol.

2. The model proposed in [1] does not provide a closed form analytical formulation for the number of queries and the number of transmitted bits needed to identify all tags in the system. Instead, it relies on simulations and averaging to do so. To solve this problem, we formulate our proposed Markov model completely and derive the accurate analytical formulations for the number of required queries and the number of transmitted bits in EPC Gen-2 protocol (as a function of the number of tags in the system).

3. We validate the accuracy of our proposed Markov model and the formulations we derived using simulations, and compare our Markov model with the one proposed in [1]. Simulation results confirm that our proposed Markov model accurately represents the EPC Gen-2 protocol and is more accurate than the model proposed in [1].

The rest of the chapter is organized as follows: Section 5.2 explains the Q-algorithm and the EPC Gen-2 protocol. Section 5.3 discusses the state of the art model proposed by Wang *et al.* to represent the EPC Gen-2 protocol [1]. In Section 5.4, we propose a new analytical model for the EPC Gen-2 protocol based on the absorbing Markov chain systems and then we formulate this model. Performance evaluation and comparisons are presented in Section 5.5 followed by conclusions in Section 5.6.

5.2 The Standard Q-algorithm

The EPC Gen-2 protocol provides a standard communication mechanism for transferring and receiving data between RFID tags and the reader(s). It provides a wireless protocol including the physical layer and the medium access control (MAC) specifications for passive UHF RFID tags that operate in the frequency range of 860 MHz to 960 MHz. This protocol uses the dynamic framed-slotted ALOHA technique to identify the tags, and takes advantage of an adaptive algorithm called the Q-algorithm to determine the number of time slots required at each query. In the EPC Gen-2 protocol, the reader starts interrogating the tags present in its vicinity by sending a query command and a parameter called Q. Those tags that receive this query randomly choose a slot number (SN) between 0 and $2^Q - 1$. After this step, any tag whose SN is 0 generates a random 16-bit number called $RN16$ and sends it back to the reader. Since each tag randomly chooses a time slot from the possible 2^Q slots independently of the others, three scenarios may happen. In the first scenario, called the idle transmission, no tag selects 0 for its SN and the reader receives no reply from the tags. In the second scenario, called the single transmission, only one tag selects 0 for its SN and sends its $RN16$ to the reader. The reader receives this $RN16$ and informs all the tags that only the tag with this $RN16$ is allowed to use the wireless channel and to send its ID to the reader. As a result, this tag successfully sends its ID to the reader while all other tags remain silent. In the third scenario, called the collided transmission, more than one tag selects 0 for their SN. As a result, more than one tag sends $RN16$ to the reader and therefore collision happens. If collision happens, the transmission fails [3].

As can be inferred from the above, the Q parameter plays a significant role in the EPC Gen-2 protocol. If Q is relatively large and the number of tags is small, the chance of idle transmission increases. On the other hand, if Q is relatively small while the number of tags in the system is large, the chance of collided transmission increases. Therefore, the Q

parameter should be chosen wisely to reduce the chance of idle or collided transmissions. The EPC Gen-2 protocol uses the adaptive Q-algorithm to change the value of Q (and therefore the number of available time slots) based on the responses the reader receives from the tags. Fig. 5.1 shows how the adaptive Q-algorithm works. Here, Q is a parameter used by the EPC Gen-2 protocol to indicate the number of available time slots to the tags and Q_{fp} is the floating-point representation of Q. There is also another parameter c which is used to adjust the rate of changing Q in the Q-algorithm. The value of Q_{fp} is initialized to 4, and c can be selected from 0.1 to 0.5 by the system designer. An integrator typically uses small values of c when Q is large and large values of c when Q is small [3]. When a query command is sent to the tags, the value of Q_{fp} is rounded to the nearest integer and this rounded value is assigned to Q. Then, the value of Q is sent to the tags along with the query command. Each tag chooses a random SN according to the value of Q and replies to the reader. If an idle transmission happens, the Q-algorithm decreases the value of Q_{fp} by c, truncates the new Q_{fp} to the nearest integer and adjusts the value of Q for the next query command accordingly. If a single transmission happens, the Q-algorithm does not change the value of Q_{fp} and uses the previous Q for the next query command. However, if a collision happens, the Q-algorithm increases the value of Q_{fp} by c and adjusts the new Q accordingly for the next query command. It should be noted that the value of Q cannot be less than 0 or greater than 15. This procedure continues until all the tags in the system are identified successfully by the reader. Using the above mechanism, the Q-algorithm changes the number of time slots dynamically and controls the tag identifying process based on the number of tags in the system and their responses to the reader's queries.

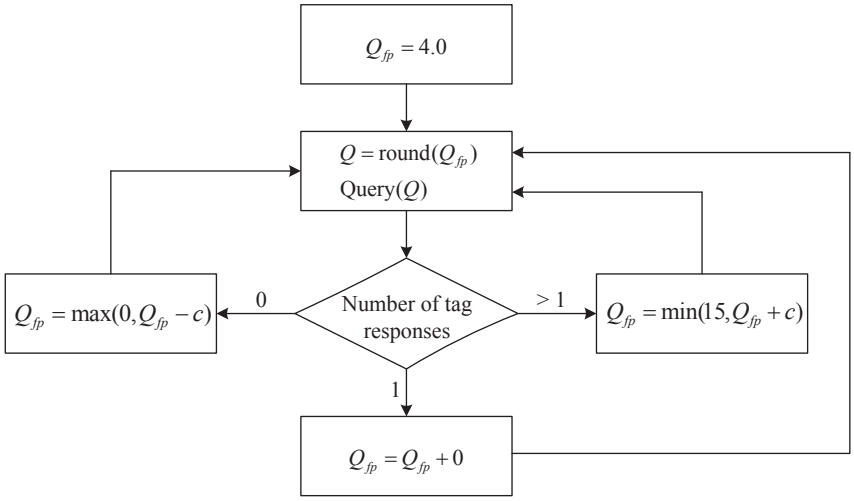

Figure 5.1: The adaptive Q-algorithm used by EPC Gen-2 [3].

5.3 The Model Proposed by Wang *et al.* [1]

In this section, we explain the model proposed by Wang *et al.* for analysing the performance of the EPC Gen-2 protocol [1]. The EPC Gen-2 protocol is modeled as a Markov chain in [1]. We denote this model by the first Markov chain (FMC) model for the EPC Gen-2 protocol. In this model, n shows the current number of unidentified tags in the system, N stands for the initial number of tags in the system, and Q is the parameter used by the reader to inform the tags about the number of available time slots as explained in Section 5.2. In the FMC model, the pair of Q and n is shown by (Q, n) and it is called a state.

In the FMC model, single transmissions are shown by S. After a single transmission, the system jumps from state (Q, n) to state $(Q, n-1)$. This is exactly the same as what happens in the actual Q-algorithm after a single transmission. If the system is in state $(Q, 1)$ and a single transmission happens, it jumps to state $(Q, 0)$ and remains there, meaning that the query process has finished successfully. However, the story is a little different for the idle and collided transmissions. If an idle transmission happens, n is not

changed but Q_{fp} is decreased by c in the actual Q-algorithm. This, on the other hand, may result in two different events. The Q parameter is decreased by 1 if the new Q_{fp} is closer to $Q-1$ than to Q. However, the Q parameter is not changed if Q_{fp} is still closer to Q than to $Q-1$. In other words, the value of Q may or may not change after an idle transmission. On the other hand, there is no Q_{fp} parameter in the FMC model and everything is explained by Q and n. To reflect the effect of changing Q_{fp} on Q, Wang *et al.* assume that after an idle transmission, the value of Q is decreased by 1 with probability P_{I1} or it is not changed with probability P_{I0}, where I shows the idle transmission, 0 shows that Q is not decreased and 1 indicates that Q is decreased by 1. We have the same story for collided transmissions. Again, a collided transmission may result in increasing the value of Q by 1 if the new Q_{fp} is closer to $Q+1$ than to Q, or it may result in the same value of Q if the new Q_{fp} is closer to Q than to $Q+1$. However, in the FMC model it is assumed that after a collided transmission, the value of Q is either increased by 1 with probability P_{C1} or it is not changed with probability P_{C0} [1].

In the FMC model, the probability of single transmission $P_S(Q,n)$ is calculated as

$$P_S(Q,n) = n \times \left(\frac{1}{2^Q}\right) \times \left(1-\frac{1}{2^Q}\right)^{n-1} \tag{5.1}$$

and $P_{I0}(Q,n)$ and $P_{I1}(Q,n)$ are calculated as

$$P_{I0}(Q,n) = P_{0|I}(Q,n) \times P_I(Q,n) \tag{5.2}$$

$$P_{I1}(Q,n) = P_{1|I}(Q,n) \times P_I(Q,n) \tag{5.3}$$

where $P_I(Q,n)$ is the probability of idle transmission and it is calculated as below

$$P_I(Q,n) = \left(1 - \frac{1}{2^Q}\right)^n . \tag{5.4}$$

As can be seen, the $P_{0|I}(Q,n)$ and $P_{1|I}(Q,n)$ probabilities are also needed to calculate $P_{I0}(Q,n)$ and $P_{I1}(Q,n)$. In order to calculate $P_{0|I}(Q,n)$ and $P_{1|I}(Q,n)$, Wang *et al.* use the following assumption: "*In long run, for each update triggered by an idle transmission, Q is decremented by 1 with probability c and is not changed with probability* $(1-c)$" [1]. Using this assumption

$$P_{0|I}(Q,n) = 1 - c \tag{5.5}$$

$$P_{1|I}(Q,n) = c\,. \tag{5.6}$$

Similarly, P_{C0} and P_{C1} are calculated as below

$$P_{C0}(Q,n) = P_{0|C}(Q,n) \times P_C(Q,n) \tag{5.7}$$

$$P_{C1}(Q,n) = P_{1|C}(Q,n) \times P_C(Q,n) \tag{5.8}$$

where the probability of collided transmission $P_C(Q,n)$ is calculated as below

$$P_C(Q,n) = 1 - P_S(Q,n) - P_I(Q,n). \tag{5.9}$$

As in the idle scenario, $P_{0|C}(Q,n)$ and $P_{1|C}(Q,n)$ are needed to calculate $P_{C0}(Q,n)$ and $P_{C1}(Q,n)$. To calculate these probabilities, Wang *et al.* use the following assumption: "*In long run, for each update triggered by a collided transmission, Q is incremented by 1 with*

probability c and is not changed with probability $(1 - c)$" [1]. Using this assumption

$$P_{0|C}(Q, n) = 1 - c \tag{5.10}$$

$$P_{1|C}(Q, n) = c \, . \tag{5.11}$$

Details on how Eq. (5.1) to (5.11) are derived can be found in [1].

The FMC model provides a novel way of modeling the EPC Gen-2 protocol. Simulation results show that this model can predict the behavior of the EPC Gen-2 protocol, and confirm the usefulness of the FMC model. However, there exist two concerns which can be noted here and solving these concerns will add to the value and usefulness of the FMC model. The first concern is the approximation used in this model. In the FMC model, the EPC Gen-2 protocol is modeled using the Q and n parameters but Q originally depends on Q_{fp}, and Q_{fp} is not reflected in the FMC model. As a result, the FMC model is always an approximation of the EPC Gen-2 protocol. The second concern is the mathematical formulation of the FMC model. While the Markov chain model proposed in [1] can predict the behavior of the EPC Gen-2 protocol in real RFID systems very well, it does not provide an explicit mathematical formulation for the number of queries needed to identify all tags in the system (or similarly the time needed to identify all tags). This model also does not give an explicit mathematical formulation for the total number of bits transmitted by all tags in the system. In other words, the FMC model can predict the behavior of the EPC Gen-2 protocol using simulations, but it does not provide a mathematical formulation to predict the behavior of the protocol directly. This model depends on simulation results, and simulations are always time consuming, especially when we want to study a typical RFID system with thousands of tags. Moreover, we need to increase the number of repetitions

and averaging to increase the accuracy of the FMC model. We would be able to predict the behavior of the EPC Gen-2 protocol directly and without needing the time consuming simulations if we can provide explicit mathematical formulations for the proposed Markov chain model. Considering the above facts and concerns, we provide a more accurate and useful analytical model for the EPC Gen-2 protocol.

5.4 The New Analytical Framework

The idea of modeling the EPC Gen-2 protocol as a Markov chain system was first suggested in [1]. We referred to this model as the first Markov chain (FMC) model for the EPC Gen-2 protocol. In this section, we modify the FMC model and propose a new analytical model for the EPC Gen-2 protocol. We name our proposed analytical model the second Markov chain (SMC) model for the EPC Gen-2 protocol. Although we use the same approach as the one used in [1], our proposed SMC model has two main differences with the FMC model. First, the FMC model uses Q and n as the two parameters of the Markov chain system while in our SMC model, Q_{fp} and n play the roles of the two key parameters in the system as is now discussed. In the EPC Gen-2 protocol, Q originally depends on Q_{fp}, but Q_{fp} is not reflected in the FMC model [1]. In the FMC model, the Q parameter is always an approximation of the actual Q in the Q-algorithm, and the behavior of the FMC model is always an approximation of the behavior of the EPC Gen-2 protocol. The effects of this inaccuracy will be shown in more detail in Section 5.5. Our proposed SMC model, on the other hand, uses the Q_{fp} parameter and thus, it can always provide an accurate representation of the EPC Gen-2 protocol. The second difference is even more important. The FMC model does not provide any mathematical formulation for the average number of queries required (or equivalently, the average time needed) to identify all tags in the system using the EPC Gen-2 protocol. Instead, the FMC model relies on simulations to do so

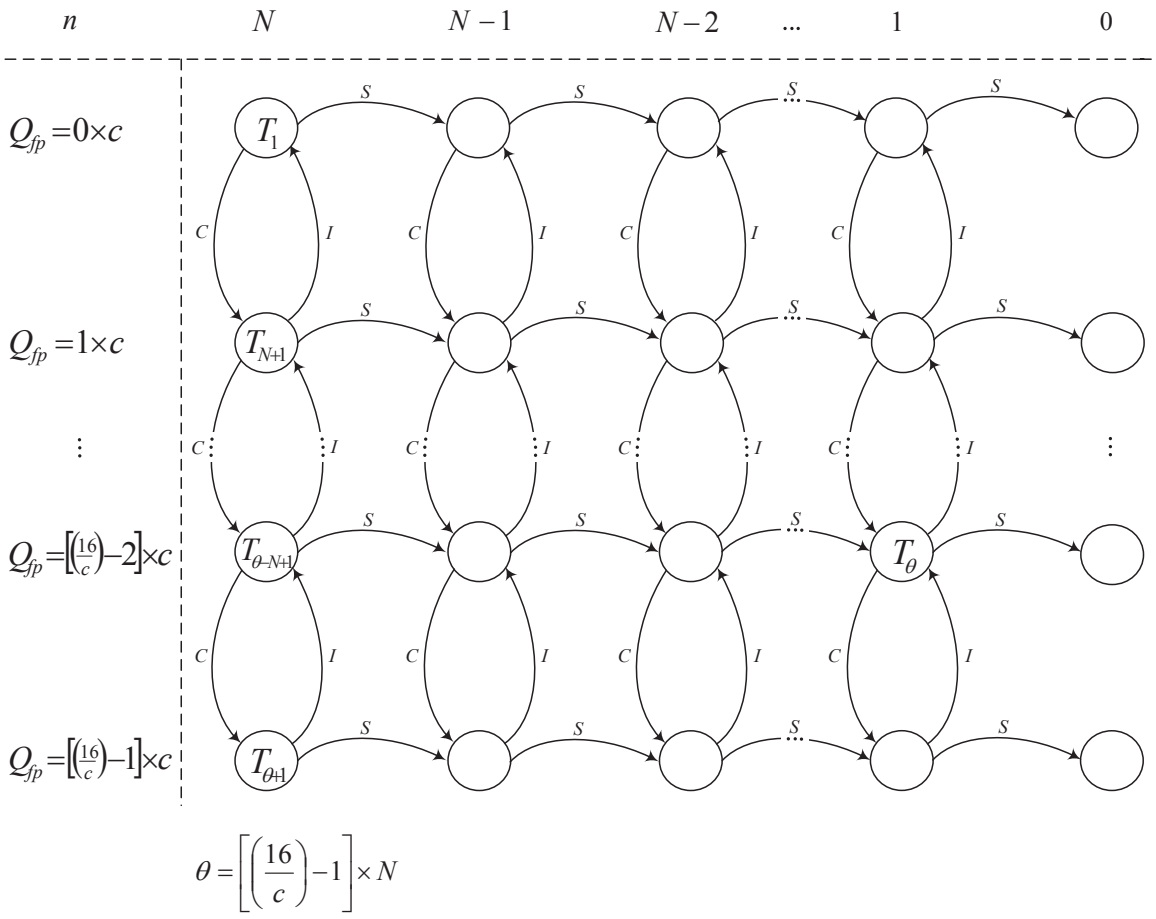

Figure 5.2: Our proposed SMC model.

and to predict the behavior of the EPC Gen-2 protocol. We, on the other hand, not only propose the accurate SMC model for the EPC Gen-2 protocol, but also mathematically formulate it using the absorbing Markov chain theorem. In other words, we do not need to simulate the SMC model and average the simulation results to study the behavior of the EPC Gen-2 protocol. Instead, we can calculate all the required parameters directly using the mathematical formulation provided.

The proposed SMC model is shown in Fig. 5.2 as a two dimensional absorbing Markov chain. In this model, n shows the current number of tags in the system, N stands for the initial number of tags in the system, Q_{fp} and c are as defined in Section 5.2. We also define

θ as $\left[\left(\frac{16}{c}\right) - 1\right] \times N$ to save space in Fig. 5.2. Using Q_{fp} and n as the parameters of our Markov chain, we have $\left[(N+1) \times \left(\frac{16}{c}\right)\right]$ states for each EPC Gen-2 RFID system with N tags. These states are shown by T_i in Fig. 5.2 where i varies between 1 to $\left[\left(\frac{16}{c}\right) \times (N+1)\right]$. As can be seen in Fig. 5.2, n is decreased from left to right, and Q_{fp} is increased from top to bottom. The EPC Gen-2 protocol starts from N tags in the system and eventually ends up to a state with 0 tags. In the actual Q-algorithm, three scenarios of single, idle and collided transmissions may happen as explained in Section 5.2. In Fig. 5.2, single, idle and collided transmissions are shown by S, I and C, respectively. After a single transmission, the system jumps from state (Q_{fp}, n) to state $(Q_{fp}, n-1)$. If the system is in state $(Q_{fp}, 1)$ and a single transmission happens, it jumps to state $(Q_{fp}, 0)$ and remains there, meaning that the query process has finished successfully. These states are called absorbing states. Our proposed model is an absorbing Markov model because the EPC Gen-2 protocol is finally absorbed in one of the rightmost states ($n = 0$). If an idle transmission happens, n is not changed but Q_{fp} is decreased by c, and the system jumps to the corresponding state. If a collision occurs, n is not changed but Q_{fp} is increased by c, and the system jumps to the state with the same n and the new Q_{fp}. Using this model, the EPC Gen-2 protocol cannot stay in any of the states after a query command. This is exactly what actually happens in real EPC Gen-2 protocol. This is one of the differences between our proposed SMC model and the FMC model proposed in [1]. In the FMC model, each state can have two separate feedback loops corresponding to idle and collided transmissions. Each feedback loop starts and ends at the same state. In other words, the system may remain in the same state after an idle or collided transmission in the FMC model. However, in a real RFID system and in our proposed SMC model, it is not possible that the system remains in the same state after a query message.

5.4.1 Expected Number of Required Queries

In order to easily formulate the SMC model, we arrange the order and indices of T_i states such that we can divide them into two separate groups, called the transient states and the absorbing states. In Fig. 5.2, the first N columns show the transient states, T_1 to $T_{\left(\frac{16}{c}\right)\times N}$, and the rightmost column shows the absorbing states, $T_{\left(\frac{16}{c}\right)\times N+1}$ to $T_{\left(\frac{16}{c}\right)\times (N+1)}$. Using the SMC model, the probability of a single transmission is calculated as

$$P_S(Q,n) = n \times \left(\frac{1}{2^Q}\right) \times \left(1 - \frac{1}{2^Q}\right)^{n-1}, \tag{5.12}$$

and the probability of idle and collided transmissions are calculated using Eq. (5.13) and (5.14)

$$P_I(Q,n) = \left(1 - \frac{1}{2^Q}\right)^{n} \tag{5.13}$$

$$P_C(Q,n) = 1 - P_S(Q,n) - P_I(Q,n)\ . \tag{5.14}$$

Now, we write the transition matrix of the Markov system shown in Fig. 5.2 as below

$$\mathbf{P} = \begin{array}{c} \\ \text{Tr.} \\ \\ \text{Abs.} \end{array} \begin{array}{c} \begin{array}{cc} \text{Tr.} & \text{Abs.} \end{array} \\ \left[\begin{array}{c|c} \mathbf{G} & \mathbf{H} \\ \hline \mathbf{0} & \mathbf{I} \end{array}\right] \end{array}$$

where $\mathbf{P}$ is the transition matrix, $p_{i,j}$ shows the probability of transition from state T_i to state T_j, $\mathbf{G}$ is the matrix of transient states, $\mathbf{H}$ is the matrix of the absorbing states, $\mathbf{0}$ is the zero matrix and $\mathbf{I}$ is the identity matrix. Using this notation and assuming that $\mu = \frac{16}{c}$ and $\nu = \left(\frac{16}{c}\right) \times N$, the size of $\mathbf{P}$, $\mathbf{G}$, $\mathbf{H}$, $\mathbf{0}$ and $\mathbf{I}$ matrices are $(\mu+\nu)\times(\mu+\nu)$, $\nu \times \nu$,

$\nu \times \mu$, $\mu \times \nu$ and $\mu \times \mu$, respectively. From the Markov chain theorem, we know that the probability of the system being in the transient state T_j after x jumps and having started from the transient state T_i is given by $g_{i,j}^x$, where $g_{i,j}^x$ is the i,jth component of matrix $\mathbf{G}^x$. The following specifications of the $\mathbf{G}$ matrix are critical in providing an analytical framework for the EPC Gen-2 protocol.

Lemma 1: If the number of jumps (transitions) tends to infinity, then $\lim_{x\to\infty} \mathbf{G}^x = 0$.

Proof: From each transient state T_j, it is possible to reach an absorbing state. Let s_j be the minimum number of steps needed to reach an absorbing state starting from T_j. Let ρ_j be the probability that starting from T_j, the process does not reach an absorbing state in s_j steps. Then, $\rho_j < 1$. Let s_{max} be the largest of s_j and ρ_{max} be the largest of ρ_j. The probability of not being absorbed in s_{max} steps is always less than or equal to ρ_{max}, in $2s_{max}$ steps is always less than or equal to ρ_{max}^2, etc. Since $\rho_{max} < 1$, $\lim_{x\to\infty} \rho_{max}^x = 0$. Since the probability of not being absorbed in n steps is monotone decreasing, $\lim_{x\to\infty} \mathbf{G}^x = 0$. ■

Lemma 2: In the SMC model, $(\mathbf{I} - \mathbf{G})^{-1}$ always exists, where $\mathbf{I}$ is the corresponding identity matrix of the same size as $\mathbf{G}$.

Proof: We assume that there exists a matrix γ that results in $(\mathbf{I} - \mathbf{G}) \times \gamma = 0$, thus $\gamma = \mathbf{G} \times \gamma$. By repeating the same procedure, we have $\gamma = \mathbf{G}^x \times \gamma$. On the other hand, we have $\lim_{x\to\infty} \mathbf{G}^x = 0$ from the first lemma. Therefore, $\lim_{x\to\infty} \gamma = \lim_{x\to\infty} \mathbf{G}^x \times \gamma = 0$ which is the only obvious solution for $(\mathbf{I} - \mathbf{G}) \times \gamma = 0$. Thus, $(\mathbf{I} - \mathbf{G})^{-1}$ always exists. ■

Now we can use these two lemmas to formulate our SMC model. Using the second lemma, we can define a matrix $\mathbf{M}$ as below

$$\mathbf{M} = (\mathbf{I} - \mathbf{G})^{-1} . \tag{5.15}$$

We also have

$$\mathbf{I} - \mathbf{G}^{x+1} = (\mathbf{I} - \mathbf{G}) \times (\mathbf{I} + \mathbf{G} + \mathbf{G}^2 + \mathbf{G}^3 + ... + \mathbf{G}^x) \ . \tag{5.16}$$

Multiplying both sides by $\mathbf{M}$, we have

$$\begin{aligned} \mathbf{M} \times (\mathbf{I} - \mathbf{G}^{x+1}) = (\mathbf{I} - \mathbf{G})^{-1} \times (\mathbf{I} - \mathbf{G}) \\ \times (\mathbf{I} + \mathbf{G} + \mathbf{G}^2 + \mathbf{G}^3 + ... + \mathbf{G}^x) \ . \end{aligned} \tag{5.17}$$

From the first lemma we have $\lim_{x\to\infty} \mathbf{G}^x = 0$, so by letting x tend to infinity we have

$$\mathbf{M} = (\mathbf{I} + \mathbf{G} + \mathbf{G}^2 + \mathbf{G}^3 + ...) \tag{5.18}$$

or equivalently,

$$m_{i,j} = g_{i,j}^0 + g_{i,j}^1 + g_{i,j}^2 + ... \ . \tag{5.19}$$

Now let T_i and T_j be two transient states, and $\alpha_{i,j}(k)$ be a random variable which equals 1 if the absorbing Markov chain of Fig. 5.2 reaches state j after exactly k jumps and starting from state i, and $\alpha_{i,j}(k)$ equals 0 otherwise. According to matrix $\mathbf{G}$ we have

$$Pr(\alpha_{i,j}(k) = 1) = g_{i,j}^k \tag{5.20}$$

$$Pr(\alpha_{i,j}(k) = 0) = 1 - g_{i,j}^k \tag{5.21}$$

where $g_{i,j}^k$ is the i,jth entry of $\mathbf{G}^k$. The expected number of times that the absorbing Markov chain is in state T_j in the first k steps, given that it starts from state T_i is

$$\begin{aligned} & E\{\alpha_{i,j}(0) + \alpha_{i,j}(1) + \alpha_{i,j}(2) + ... + \alpha_{i,j}(k)\} \\ &= E\{\alpha_{i,j}(0)\} + E\{\alpha_{i,j}(1)\} + ... + E\{\alpha_{i,j}(k)\} \\ &= g_{i,j}^0 + g_{i,j}^1 + g_{i,j}^2 + ... + g_{i,j}^k \ . \end{aligned} \tag{5.22}$$

Letting k tend to infinity, we have

$$\begin{aligned} & E\{\alpha_{i,j}(0) + \alpha_{i,j}(1) + \alpha_{i,j}(2) + ...\} \\ &= g_{i,j}^0 + g_{i,j}^1 + g_{i,j}^2 + ... \ . \end{aligned} \tag{5.23}$$

Finally from Eq. (5.19) and (5.23), we have

$$E\{\alpha_{i,j}(0) + \alpha_{i,j}(1) + \alpha_{i,j}(2) + ...\} = m_{i,j} \tag{5.24}$$

where $m_{i,j}$ is the i,jth entry of matrix $\mathbf{M}$ defined in Eq. (5.15). Based on the above, if the EPC Gen-2 protocol starts from state i, the expected number of times that it visits state j before all the tags in the system are identified and the EPC Gen-2 protocol is terminated can be calculated using Eq. (5.24). We know that the EPC Gen-2 protocol always starts with Q_{fp} equals to 4 [3]. Knowing this fact and using the SMC model shown in Fig. 5.2, we can simply conclude that the EPC Gen-2 protocol always starts from state $T_{4\times\left(\frac{1}{c}\right)\times N+1}$. Therefore, we can calculate the expected number of queries in the EPC Gen-2 protocol given the number of tags at the beginning by calculating and adding the number of visits to each of the transient states. In other words, the expected number of queries in the EPC Gen-2 protocol is calculated by adding all entries of the $(4 \times \left(\frac{1}{c}\right) \times N + 1)$th row in the $\mathbf{M}$

matrix as below

$$\overline{q} = \sum_{j=1}^{\left(\frac{16}{c}\right)\times N} m_{\left(4\times\left(\frac{1}{c}\right)\times N+1\right),j} \tag{5.25}$$

where $\overline{q}$ shows the average number of queries required to identify all of the N tags in the system.

Using the above formulation, there is no need to run multiple simulations and average them to obtain the number of required queries as done in [1], instead, we can simply use Eq. (5.25) and calculate $\overline{q}$ directly. As we will see in Section 5.5, the simulation results perfectly confirm the proposed SMC model and its formulation.

5.4.2 Expected Number of Transmitted Bits

After deriving the analytical formulation for the expected number of queries in the EPC Gen-2 protocol, we derive the analytical formulation for the aggregate number of bits that are sent by the tags, before they are successfully identified by the reader. According to [3], we assume that each idle transmission results in 0 transmitted bits, each single transmission results in 16 bits for $RN16$ and 96 bits for the tag serial number (112 bits in total), and each collided transmission results in only 16 bits for $RN16$. First, we find the probability that the EPC Gen-2 protocol starts the interrogation from the transient state T_i and ends up in the absorbing state T_j. This probability is denoted by $b_{i,j}$. Using the Markov model shown in Fig. 5.2 we have

$$
\begin{aligned}
b_{i,j} &= \sum_{k=0}^{\infty} \sum_{r=1}^{\left(\frac{16}{c}\right)\times N} g_{i,r}^{k} \times h_{r,j} \\
&= \sum_{r=1}^{\left(\frac{16}{c}\right)\times N} \left[\sum_{k=0}^{\infty} g_{i,r}^{k}\right] \times h_{r,j} \\
&= \sum_{r=1}^{\left(\frac{16}{c}\right)\times N} m_{i,r} \times h_{r,j} \\
&= (\mathbf{M} \times \mathbf{H})_{i,j}
\end{aligned} \tag{5.26}
$$

where $h_{r,j}$ is the probability of jumping from the transient state T_r to the absorbing state T_j, and $m_{i,r}$ is calculated using Eq. (5.15). Therefore, we can define matrix $\mathbf{B}$ as

$$\mathbf{B} = \mathbf{M} \times \mathbf{H} \tag{5.27}$$

where $\mathbf{M}$ is calculated using Eq. (5.15) and $\mathbf{H}$ is a subset of the transition matrix $\mathbf{P}$ which shows the transition probabilities from the transient states to the absorbing states. In the EPC Gen-2 protocol, the query process always starts from state $T_{\left(4\times\left(\frac{1}{c}\right)\times N+1\right)}$, therefore, we can simply replace i with $\left(4 \times \left(\frac{1}{c}\right) \times N + 1\right)$ in Eq. (5.26).

In order to calculate the expected number of transmitted bits before all the tags are identified by the reader, we need to calculate the expected number of idle, single and collided transmissions during the tag identifying process. The aggregation of the expected number of idle, single and collided queries should equal the expected number of queries, therefore,

$$\overline{I} + \overline{S} + \overline{C} = \overline{q}\ . \tag{5.28}$$

In the EPC Gen-2 protocol, the expected number of single transmissions always equals the initial number of tags in the system. This gives us the second equation needed for deriving

$\overline{I}$, $\overline{S}$ and $\overline{C}$

$$\overline{S} = N \ . \tag{5.29}$$

Finally, we always have

$$4 + (C(i) - I(i)) \times c = Q_{fp}(i) \tag{5.30}$$

where $I(i)$ and $C(i)$ are the number of idle and collided transmissions corresponding to the ith absorbing state. Taking the expected value in Eq. (5.30) we have

$$4 + (\overline{C} - \overline{I}) \times c = \overline{Q}_{fp} \tag{5.31}$$

where $\overline{Q}_{fp}$ is calculated as

$$\overline{Q}_{fp} = \sum_{i=\left(\frac{16}{c}\right)\times N+1}^{\left(\frac{16}{c}\right)\times(N+1)} Q_{fp}(i) \times b_{\left(\left(\frac{4}{c}\right)\times N+1\right),i} \ . \tag{5.32}$$

Solving Eq. (5.28), (5.29) and (5.31) we have

$$\begin{cases} \overline{I} = \frac{\overline{q}-N}{2} + \frac{4-\overline{Q}_{fp}}{2c} \\ \overline{S} = N \\ \overline{C} = \frac{\overline{q}-N}{2} - \frac{4-\overline{Q}_{fp}}{2c} \ . \end{cases} \tag{5.33}$$

Based on the above, we can calculate $\overline{I}$, $\overline{S}$ and $\overline{C}$ for each of the $\frac{16}{c}$ possible Q_{fp}. We know that the EPC Gen-2 protocol starts from state $T_{\left(4\times\left(\frac{1}{c}\right)\times N+1\right)}$, and we have calculated the probability that the EPC Gen-2 protocol ends up in each of the $\frac{16}{c}$ absorbing states using Eq. (5.26). Therefore, the total expected number of transmitted bits is

$$\overline{TB} = 112 \times \overline{S} + 16 \times \overline{C} \tag{5.34}$$

where $\overline{TB}$ shows the expected number of transmitted bits, and $\overline{S}$ and $\overline{C}$ are calculated using Eq. (5.33).

The expected number of transmitted bits and the expected number of required queries can provide us an estimation of the time needed to detect all tags in the system using the EPC Gen-2 protocol. For example, assuming that each bit of data needs t_b milliseconds (on average) to be transmitted by the tag and received by the reader, the average required time $\overline{T}$ can be calculated as

$$\overline{T} = \overline{TB} \times t_b \tag{5.35}$$

where $\overline{TB}$ shows the expected number of transmitted bits calculated from Eq. (5.34). The same way, assuming that each round of query takes t_q milliseconds (on average), the average required time $\overline{T}$ can be calculated as

$$\overline{T} = \overline{q} \times t_q \tag{5.36}$$

where $\overline{q}$ represents the expected number of required queries calculated from Eq. (5.25).

In order to show the accuracy of our SMC model in calculating the expected number of required queries and to compare it with the FMC model, we define $Dif_{\overline{q}}$ as

$$Dif_{\overline{q}} = |\overline{q} - q_{sim}| \tag{5.37}$$

where $\overline{q}$ denotes the expected number of queries calculated using the SMC (or FMC) model and q_{sim} is the number of queries obtained from simulating a real RFID system. We also define $Dif_{\overline{TB}}$ as

$$Dif_{\overline{TB}} = |\overline{TB} - TB_{sim}| \tag{5.38}$$

where $\overline{TB}$ denotes the expected number of transmitted bits calculated using the SMC (or

FMC) model and TB_{sim} is the number of transmitted bits obtained from simulating a real RFID system. We will use Eq. (5.37) and (5.38) in Section 5.5 to show the accuracy of the proposed model and to compare it with the model proposed in [1].

5.4.3 Generalizing the SMC Model for Variable c

So far, we have modeled the EPC Gen-2 protocol based on an invariant c parameter. However, c might be a variable itself and changes as a function of the Q parameter. The EPC Gen-2 standard "recommends" using a small value of c when Q is large and a large value of c when Q is small, however, it does not suggest any criterion (or function) for changing the value of c based on the value of Q [3]. Fortunately, our proposed SMC model is a general analytical model for the EPC Gen-2 protocol and does not depend on a fixed or variable c parameter. In other words, even if c is defined as a function of Q, our SMC model will remain valid and accurate. Here, we explain how the SMC model can be generalized for RFID systems that use a variable c parameter for their tag identification process.

The Q-algorithm used in our SMC model is exactly the same as the one used by the EPC Gen-2 protocol during the tag identification process. In other words, for a fixed c in the EPC Gen-2 protocol we use the same fixed c in our SMC model and for a variable c in the EPC Gen-2 protocol we use the same variable c in our SMC model. Therefore, using a variable c parameter which changes over time based on Q does not degrade the accuracy of our proposed analytical model. It should also be noted that the structure of the proposed absorbing Markov model remains the same even if c changes over time as a function of Q. Even if c is a function of Q, the number of the states in the proposed SMC model is exactly the same as that shown in Fig. 5.2 for a fixed c. The size of the $\mathbf{G}$, $\mathbf{H}$, $\mathbf{I}$, $\mathbf{0}$ and $\mathbf{P}$ matrices are also the same as that we calculated for an invariant c. Even the $P_S(Q,n)$, $P_I(Q,n)$ and $P_C(Q,n)$ probabilities calculated using Eq. (5.12), (5.13) and (5.14) are the same for

RFID systems which operate based on a variable c. The horizontal jumps (when a single tag ID is read successfully by the reader) are the same for both RFID systems with fixed and variable c as well. The only difference between the SMC model for RFID systems with a fixed c and the SMC model for RFID systems that assume c is a function of Q is in their vertical jumps. If c is fixed during the tag identification process, vertical jumps can be from one state to another state only "one" row below (collided transmission) or "one" row above (idle transmission), while in the SMC model with a variable c, vertical jumps can be from one state to another state "few" rows below (collided transmission) or "few" rows above (idle transmission) depending on the function or criterion which changes c according to Q. The general form of the SMC model considering c as a function of Q is shown in Fig. 5.3. It should be noted that not all the vertical dotted arrows started from or ended in a state in Fig. 5.3 are used in the SMC model. Only one of the vertical dotted arrows started from (or ended in) a state happens with probability 1 if collision (or idle transmission) happens and the rest happen with probability 0. In other words, among all vertical arrows ended in (or started from) a state, the probability of one and only one of them is 1 and the rest of the jumps do not happen. To answer which vertical jump happens with probability 1 and which vertical jump happens with probability 0, we need to know c as a function of Q. If we assume that c is fixed, then the arrow started from one state can only end up at the state just one row below (above) it if collision (idle transmission) happens. This is exactly the same as Fig. 5.2. If c changes over time based on the values of Q, then the arrow started from one state ends up at a state a few rows below (above) the starting state if collision (idle transmission) happens. Based on the above, the only difference between the SMC model for a fixed c parameter and the SMC model for a variable c parameter is in their $\mathbf{G}$ matrices, but the Markov model and Eq. (5.12) to (5.38) remain exactly the same for both models. Therefore, knowing c as a function of Q, we can simply calculate

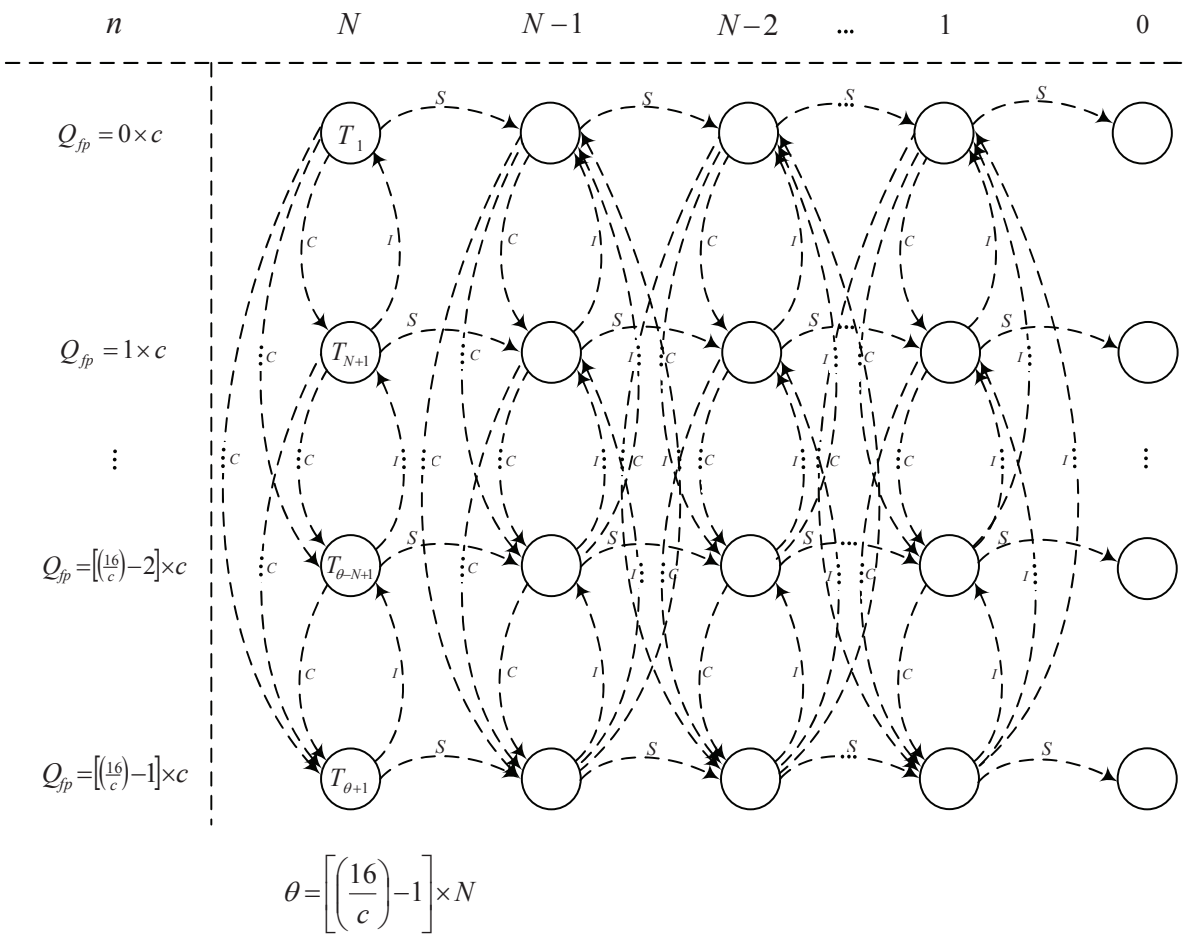

Figure 5.3: Generalized form of the SMC model for variable c.

the **G** matrix and the rest would be the same as that shown in sections 5.4.1 and 5.4.2.

In Section 5.5, we use our proposed SMC model for an RFID system which uses the function shown in Eq. (5.39) for changing c based on Q,

$$c = \begin{cases} 0.1; & Q \geq 8 \\ 0.5; & Q < 8 \end{cases} \tag{5.39}$$

and compare the average number of queries and the average number of transmitted bits obtained from simulating the real RFID system with the expected number of queries and

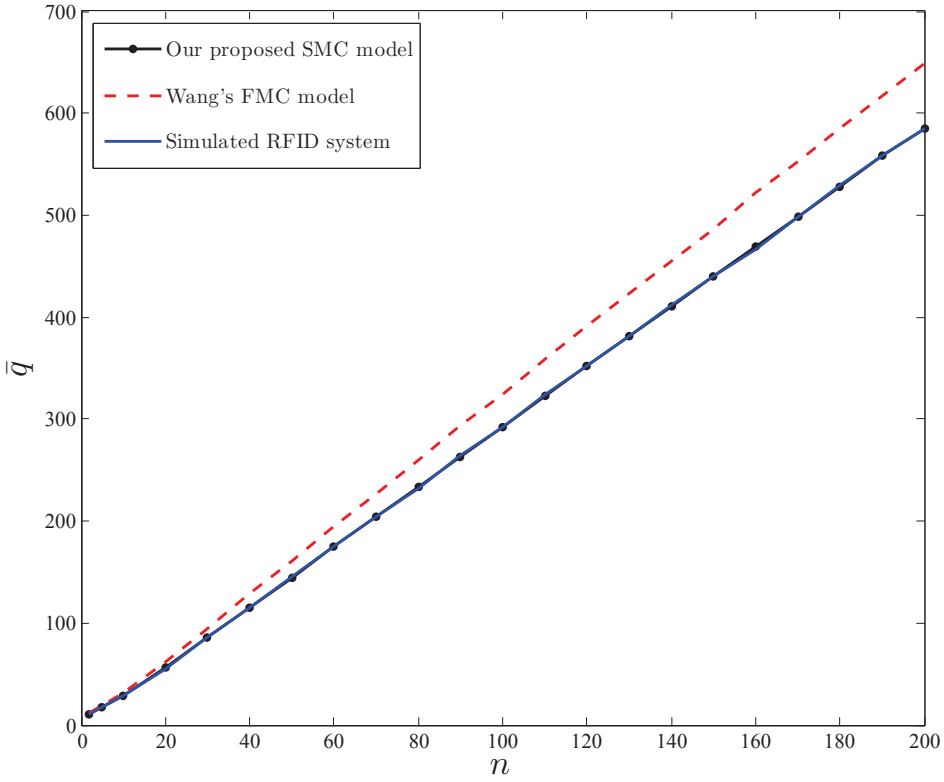

Figure 5.4: The expected number of required queries $\overline{q}$ for detecting all the tags vs. the number of tags in the system ($c = 0.2$).

the expected number of transmitted bits calculated using our proposed SMC model.

5.5 Performance Evaluation

This section presents the results of the simulation experiments we performed to evaluate the performance of our proposed SMC model. We also present the performance comparisons between the SMC model and the FMC model proposed by Wang *et al.* [1]. All simulations are performed in the MATLAB environment.

We simulated an RFID system which works based on the EPC Gen-2 protocol. We initialized c to 0.2, varied n (the number of tags in the system) between 2 and 200, and

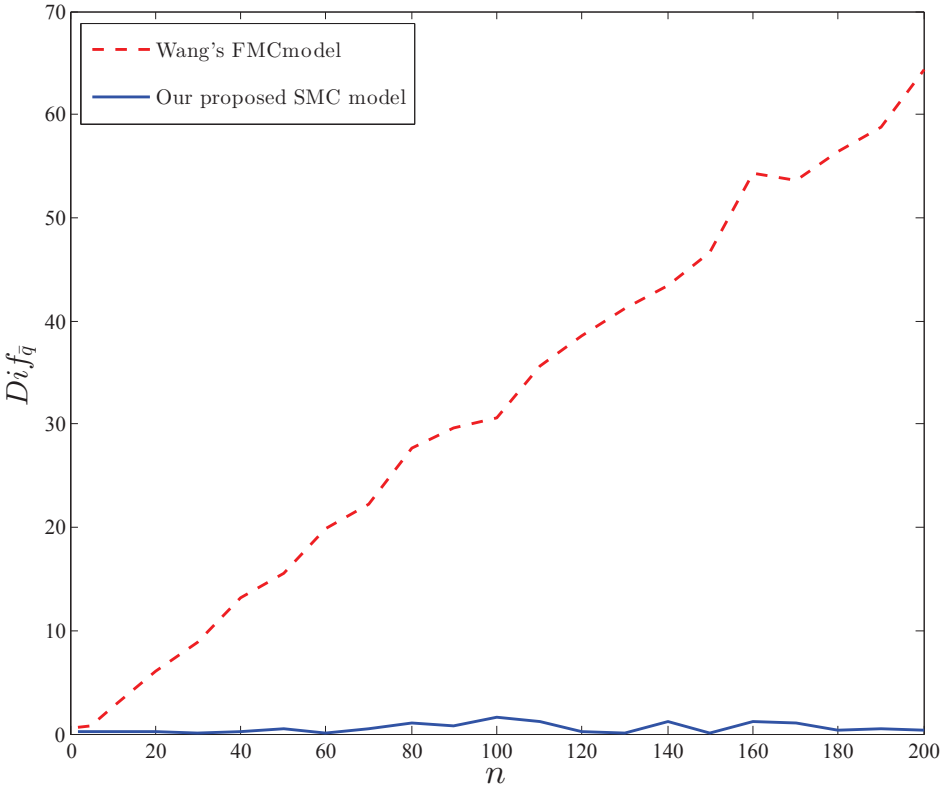

Figure 5.5: Difference between the $\overline{q}$ calculated using the FMC and SMC models and the q_{sim} obtained from the simulated RFID system ($c = 0.2$).

repeated the procedure 500 times for each n to see how many queries and how many transmitted bits are required (on average) to detect all tags in the system using the simulated EPC Gen-2 protocol. In the next step, we calculated the expected number of queries using Eq. (5.25), and the FMC model [1]. Fig. 5.4 shows the expected number of queries versus the number of tags for the simulated RFID system, our proposed SMC model and the FMC model. As can be inferred from Fig. 5.4, the proposed SMC model estimates the number of required queries accurately and the plot obtained from Eq. (5.25) almost overlaps with the plot obtained from simulating a real RFID system. The FMC model, on the other hand, can imitate the behavior of the RFID system, but the accuracy of this model decreases as the number of tags in the system increases.

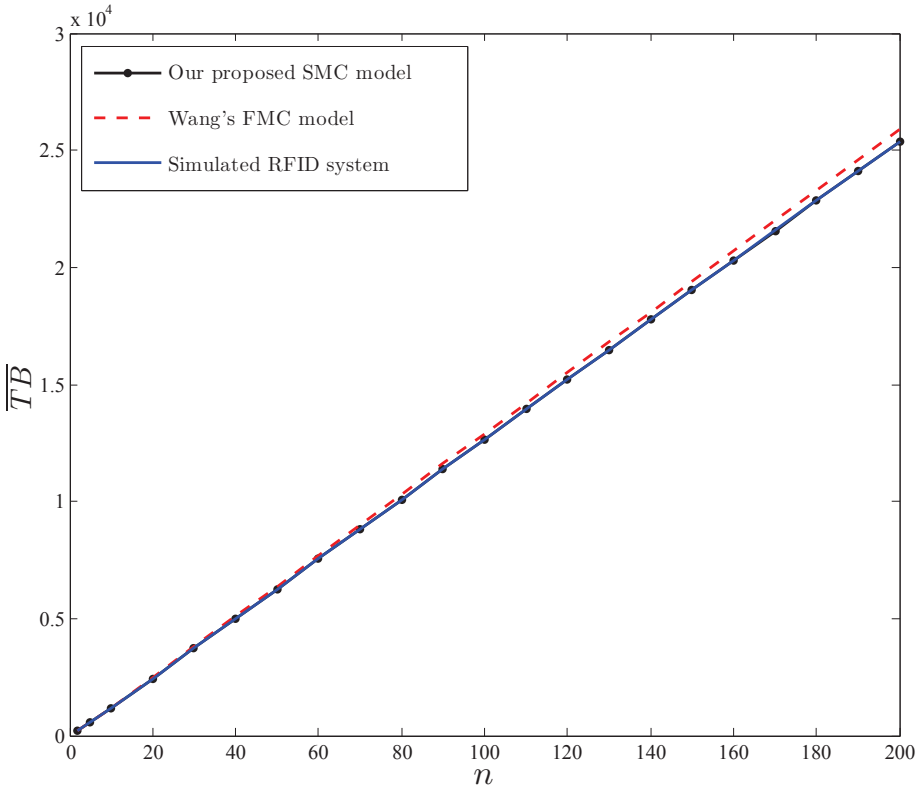

Figure 5.6: The expected number of transmitted bits $\overline{TB}$ needed for detecting all tags vs. the number of tags in the system ($c = 0.2$).

In Fig. 5.4, the two plots corresponding to our SMC model and the simulated RFID system are very close to each other so the difference between them cannot be observed easily. In Fig. 5.5, we used the $Dif_{\overline{q}}$ defined in Eq. (5.37) to better compare our proposed SMC model with the FMC model proposed in [1]. This figure shows the difference between the values estimated using our SMC model and the values obtained from the simulated RFID system, and compares it with the difference between the values obtained from the FMC model and the simulated RFID system. This figure confirms the accuracy of our proposed analytical model. It should be noted that the values calculated using Eq. (5.25) are even more accurate than the values obtained from the simulated RFID system, and if we increase the number of iterations in the simulated RFID system, the solid blue line will

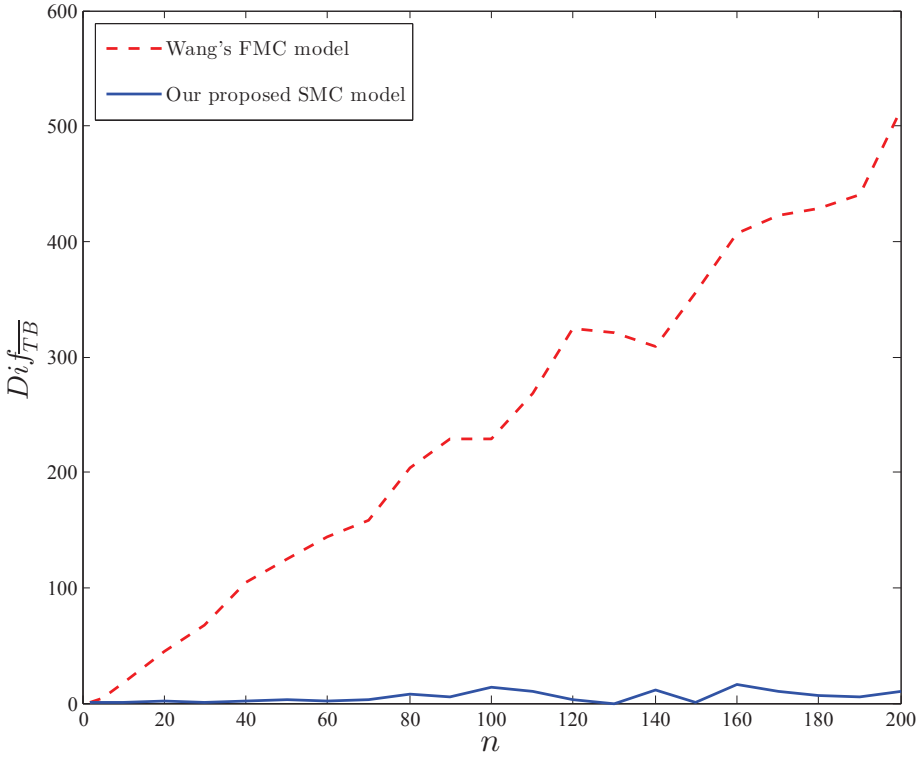

Figure 5.7: Difference between the $\overline{TB}$ calculated using the FMC and SMC models and the TB_{sim} obtained from the simulated RFID system ($c = 0.2$).

remain on the n-axis for all values of n.

After showing the accuracy of the proposed SMC model in calculating the expected number of required queries $\overline{q}$, the accuracy of the proposed SMC model in calculating the expected number of transmitted bits $\overline{TB}$ is shown in Fig. 5.6. In this figure, the expected number of transmitted bits is calculated using the SMC model, the simulated RFID system and the FMC model [1]. Again, it can be inferred from the figure that the proposed SMC model calculates the total expected number of transmitted bits more accurately compared to the FMC model. In order to better show the accuracy of the proposed SMC model, the differences between the estimated $\overline{TB}$ and the number of transmitted bits obtained from simulations are shown in Fig. 5.7 for both the SMC model and the FMC model. As can be inferred from this figure, the accuracy of the FMC model degrades as the number of tags

in the system increases and it may even have up to 500 bits of error in an RFID system with 200 tags, while the proposed SMC model remains accurate for any number of tags in the system. It should be noted that repeating the simulations and increasing the number of iterations will result in a solid blue line which is indistinguishable from the n-axis for all values of n. In other words, if we increase the number of iterations, the results obtained from the simulated RFID system would completely match the results obtained from our SMC model.

In our simulations, the only parameter that may change from one RFID system to the other is c. In order to see the effects of changing c on the accuracy of our SMC model and the FMC model, we repeated the simulations for $c = 0.4$. Fig. 5.8 shows the value of $\overline{q}$ versus n for the new c. As before, the accuracy of the model proposed in [1] decreases as the number of tags in the system increases. However, Fig. 5.9 shows that the difference between the $\overline{q}$ obtained from the FMC model and the simulated system (error) decreases a little as the value of c increases. This happens because by increasing the value of c, the rate of changing Q increases in the Q-algorithm and the system becomes less dependent on Q_{fp}. Thus, the FMC model becomes a better approximation of the real EPC Gen-2 protocol as the value of c increases.

Fig. 5.10 compares the performance of the proposed SMC model with the FMC model in terms of how accurately they calculate $\overline{TB}$ when c equals 0.4. Fig. 5.11 shows the differences between $\overline{TB}$ and TB obtained from the simulated RFID system for both the proposed SMC model and the FMC model. Again, it can be inferred from these two figures that the proposed analytical model can calculate the expected number of transmitted bits more accurately compared to the FMC model. However, the performance of the FMC model improves as the value of c increases. This happens because by increasing the value of c, the rate of changing Q increases in the Q-algorithm and the system becomes less

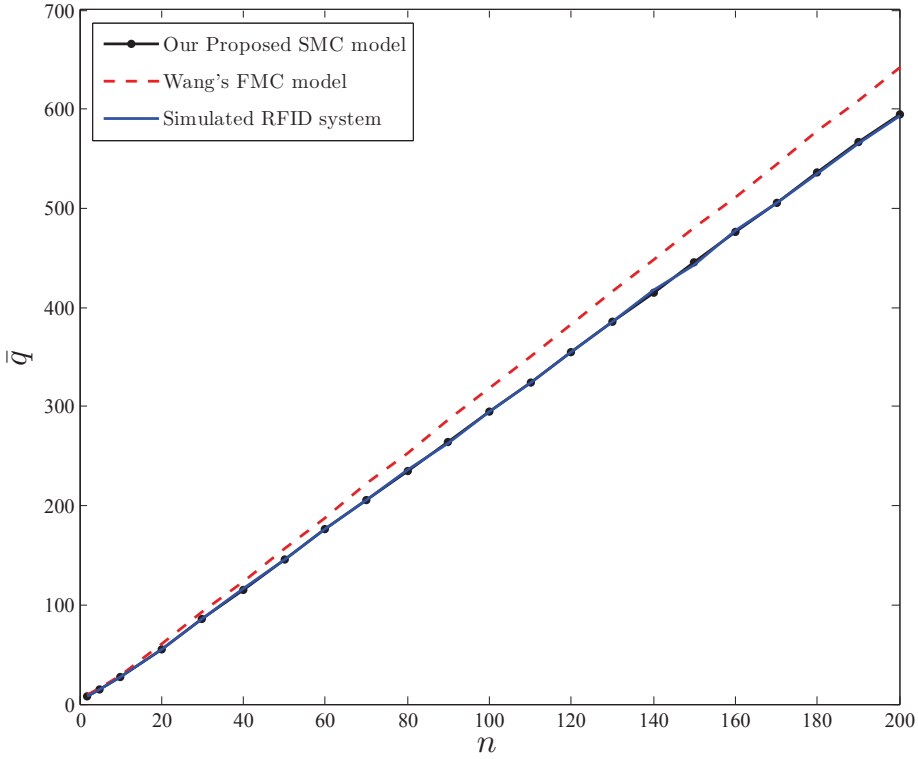

Figure 5.8: The expected number of required queries $\overline{q}$ for detecting all the tags vs. the number of tags in the system ($c = 0.4$).

dependent on Q_{fp}. However, it should be noted that our proposed SMC model always outperforms the FMC model, even for large values of c, as it is not an approximation of the EPC Gen-2 protocol.

We showed the accuracy of the proposed SMC model in estimating the expected number of queries and the expected number of transmitted bits when c does not change over time ($c = 0.2$ and $c = 0.4$). However, as mentioned in Section 5.4.3, the c parameter may not be a fixed value and it can change over time according to Q. For instance, the EPC Gen-2 standard recommends using large values of c when Q is small and small values of c when Q is large [3]. If c changes as a function of Q, we can simply use the model shown in Fig. 5.3 and repeat the same procedure as the one explained in Sections 5.4.1 and 5.4.2 to calculate the expected number of queries and the expected number of transmitted bits. We used our

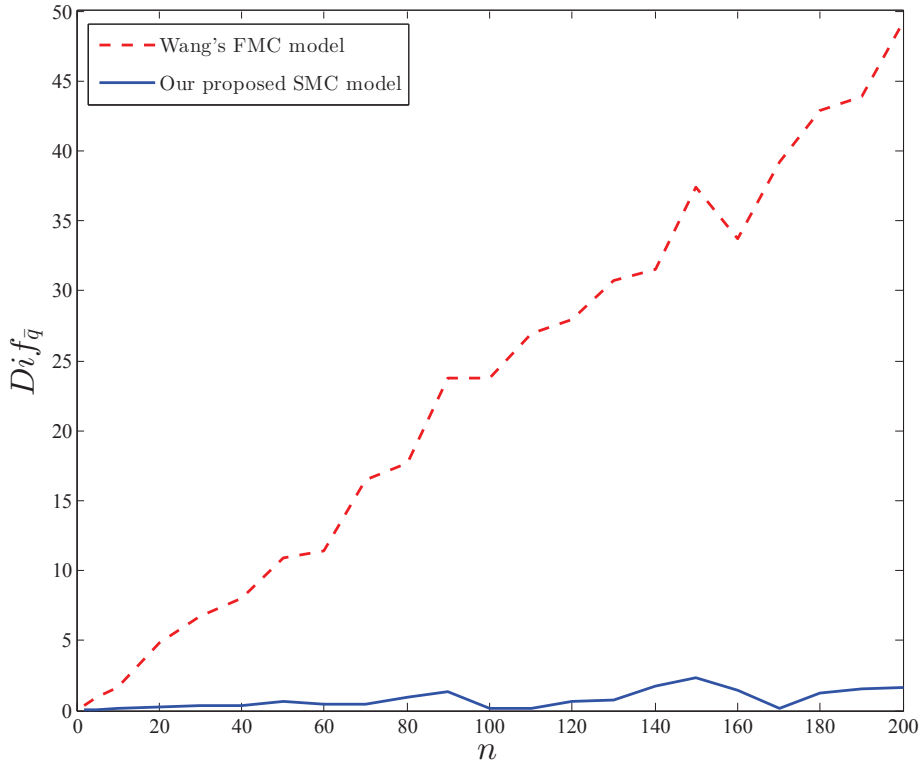

Figure 5.9: Difference between the $\overline{q}$ calculated using the FMC and SMC models and the q_{sim} obtained from the simulated RFID system ($c = 0.4$).

proposed SMC model for estimating $\overline{q}$ and $\overline{TB}$ in an RFID system which uses Eq. (5.39) for changing c during the tag identification procedure, and compared the estimated $\overline{q}$ and $\overline{TB}$ with the results obtained from simulating a real RFID system. Fig. 5.12 shows the accuracy of the proposed SMC model in estimating the expected number of queries and Fig. 5.13 shows the accuracy of the proposed method in estimating the expected number of transmitted bits. As can be inferred from Fig. 5.12 and Fig. 5.13, the proposed SMC model accurately estimates $\overline{q}$ and $\overline{TB}$ even if c is a function of Q and changes during the tag identification process.

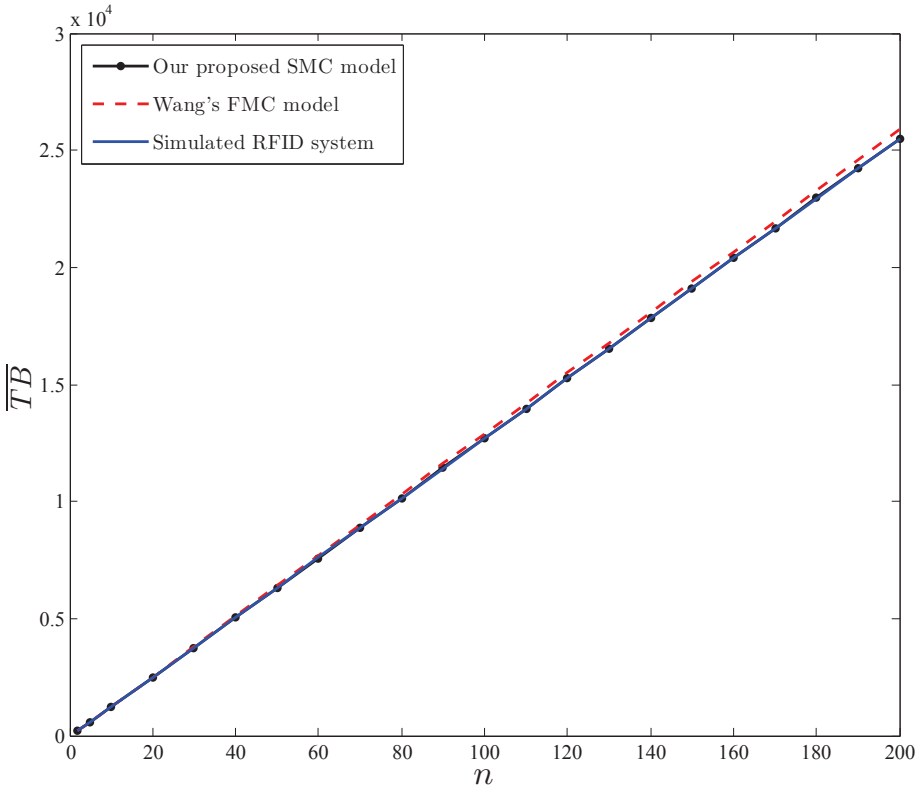

Figure 5.10: The expected number of transmitted bits $\overline{TB}$ needed for detecting all the tags vs. the number of tags in the system ($c = 0.4$).

5.6 Summary

In this chapter, we studied the standard EPC Gen-2 protocol and its tag identifying procedure which employs the Q-algorithm. Then, the FMC model proposed by Wang *et al.* was discussed [1]. We showed that the FMC model can be improved by changing the parameters of the model. Moreover, the FMC model proposed in [1] provides a novel method of studying the EPC Gen-2 protocol but it relies on extensive simulations to calculate the number of queries and the number of transmitted bits accurately.

We modeled the EPC Gen-2 protocol as an absorbing Markov chain and named it the SMC model. Using the SMC model and the analytical formulation we developed, we derived the closed form mathematical expressions for the expected number of required

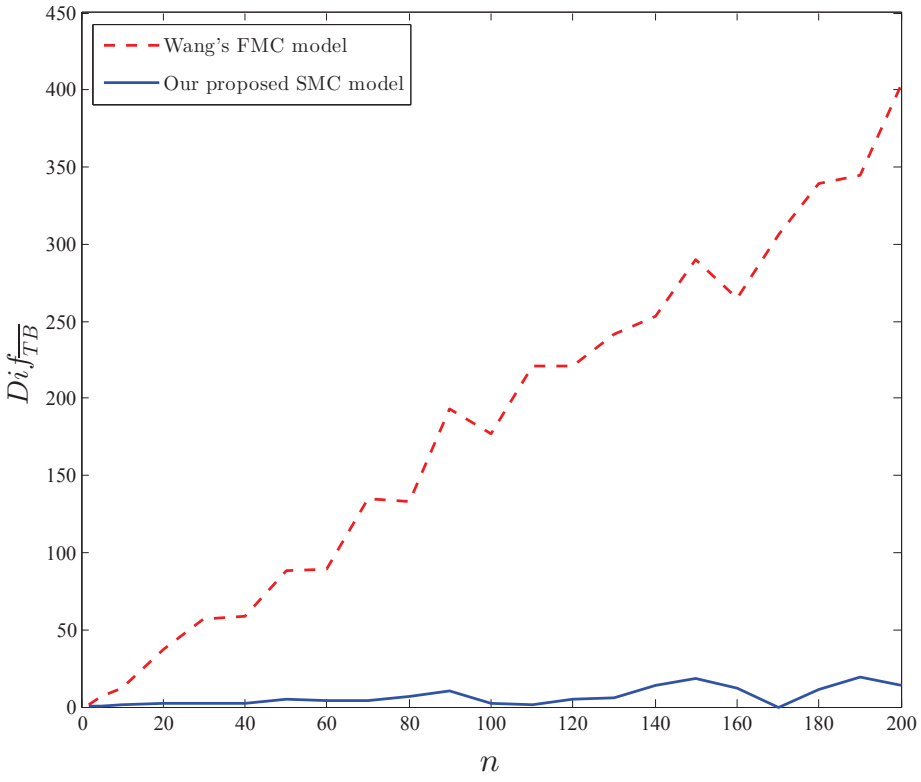

Figure 5.11: Difference between the $\overline{TB}$ calculated using the FMC and SMC models and the TB_{sim} obtained from the simulated RFID system ($c = 0.4$).

queries and the expected number of transmitted bits as a function of the number of tags in the system. These formulae enable us to calculate the number of queries and the number of transmitted bits needed to identify all tags in the system accurately and without the need of any simulation. Knowing how long each query takes on average, we can also calculate the average time needed to successfully identify all tags in the system. Using the proposed SMC model, we can also predict the values of the Q_{fp} and Q parameters in the Q-algorithm when the EPC Gen-2 protocol completes the tag identification procedure for any given c and N. Simulation results confirm that our proposed SMC model completely matches the EPC Gen-2 protocol and outperforms the model proposed in [1]. The FMC model, uses an approximation of the EPC Gen-2 protocol and its accuracy decreases as the number

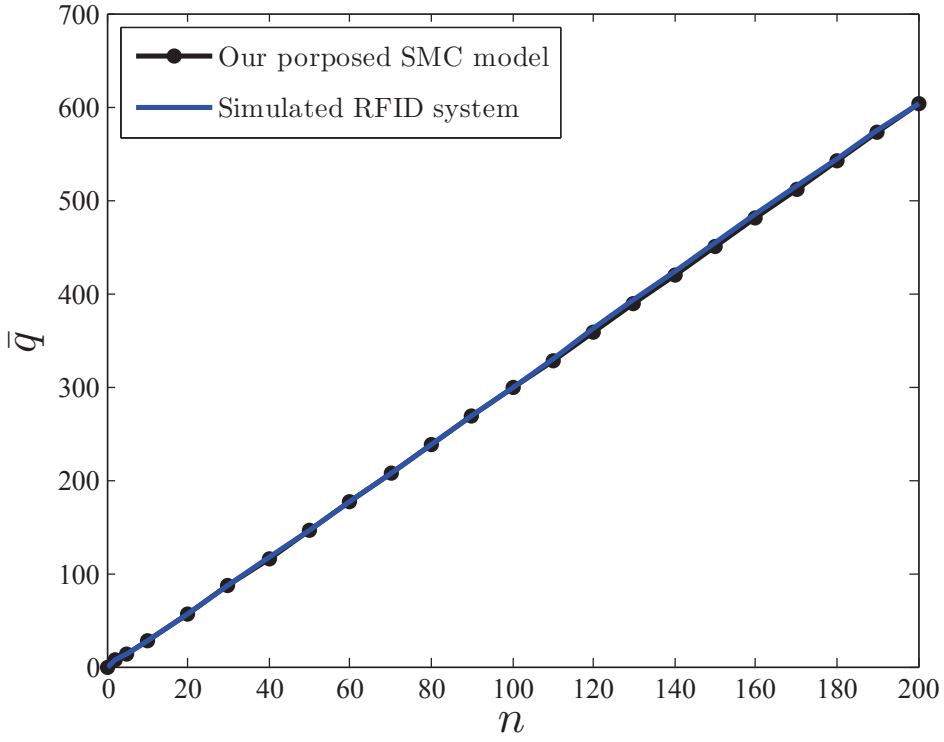

Figure 5.12: The expected number of required queries $\overline{q}$ for detecting all the tags vs. the number of tags in the system with the variable c shown by Eq. (5.39).

of tags in the system increases. Our proposed SMC model, on the other hand, is not an approximation of the EPC Gen-2 protocol and the values obtained from the mathematical expressions we derived are accurate, regardless of the number of tags in the system or any other parameter. Moreover, the FMC model has been designed for RFID systems which use a fixed c during the tag identification process. Our proposed SMC model, on the other hand, can accurately estimate the expected number of queries and the expected number of transmitted bits even if c is not fixed during the tag identification process and changes over time as a function of Q.

In this work, the proposed SMC model was used to formulate the EPC Gen-2 protocol and to calculate the expected number of queries and the expected number of transmitted bits. This analytical model, however, can be used for many other purposes such as

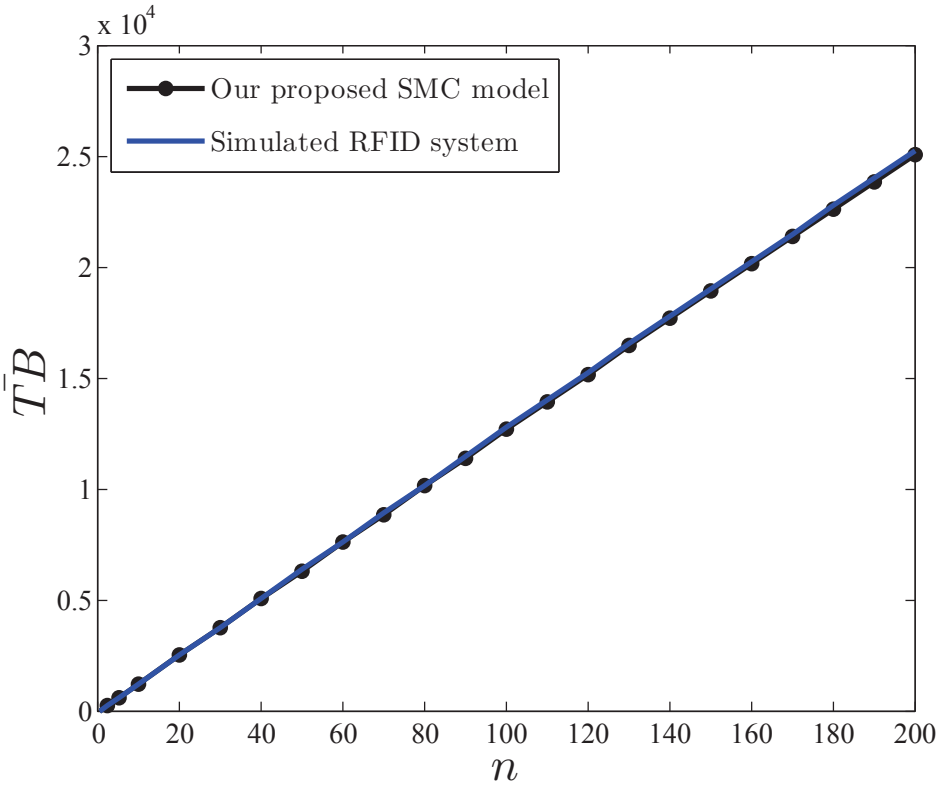

Figure 5.13: The expected number of transmitted bits $\overline{TB}$ needed for detecting all the tags vs. the number of tags in the system with the variable c shown by Eq. (5.39).

estimating the number of tags in an environment or improving the performance of RFID systems.

Chapter 6

Performance Analysis of RFID Protocols: CDMA vs. the Standard EPC Gen-2

6.1 Introduction

An RFID reader is able to communicate with a single tag at a time, yet RFID systems are prone to transmission collisions due to the shared nature of the wireless channel used by tags. To solve the collision problem, the tree-walking and the ALOHA-based anti-collision protocols have been proposed [20, 53, 55, 57, 58, 59, 83]. Recently, a framed-slotted ALOHA-based anti-collision scheme was standardized by EPCglobal [3]. This scheme is called the EPC Gen-2 protocol and allows each tag to randomly select a time slot and transmit its ID. This protocol has been accepted as the main standard for the inventory checking and supply chain management applications [1, 85].

Recently, it has been suggested by many researchers to replace the dynamic framed slotted ALOHA mechanism used by the standard EPC Gen-2 protocol with the CDMA technique to make the reader able to read more tag IDs at each query and to expedite the tag identification procedure. For instance, Mazurek suggested to use the DS-CDMA technique for active RFID tags [56], and implemented a simple RFID system in which the

tags use the DS-CDMA technique for transmission and the reader employs a non-coherent detector with successive interference cancellation [60]. Mutti and Floerkemeier suggested to replace current ALOHA-based RFID systems with CDMA-based RFID systems to prevent wasting the bandwidth during the singulation process. They focussed on the choice of the code sets that can be used and the appropriate detector for a CDMA-based RFID system. They also proposed a method for estimating the number of tags in the range of such a spread spectrum RFID system [61]. Demeechai and Siwamogsatham proposed a new tag identification protocol by modifying the standard EPC Gen-2 scheme and taking advantage of the CDMA technique in their proposed model [62]. Maina *et al.* studied typical store and warehouse environments under worst-case scenarios and recommended to employ the CDMA technique for the tag identification purpose [63]. There are few other studies that suggested the use of the CDMA technique instead of the current ALOHA-based tag identification technique employed in the standard EPC Gen-2 protocol [64, 65, 66, 67].

Although it has been advised by many researchers to take advantage of the CDMA technique and to design the new RFID protocols based on it, no analytical proof has been put forward for this idea so far. We know that the time needed to identify all tags in the system and the required bandwidth play an important role in commercial and industrial RFID systems. Therefore, we need to know whether and how the use of the CDMA technique instead of the current ALOHA-based tag identification technique would affect the time needed to identify all the tags and the bandwidth of the system. In other words, we need to know the pros and cons of using the CDMA technique for the tag identification purpose and to have a fair analytical comparison of the CDMA-based scheme with the standard EPC Gen-2 protocol before switching to the new system. In order to do that, we model the CDMA-based tag identification scheme as an absorbing Markov chain and derive the accurate analytical formulae for the expected number of queries and the total

transmitted data needed to identify all tags in the system. A similar analytical model was developed for the EPC Gen-2 protocol in Chapter 5. Using the Markov model proposed for the CDMA-based tag identification scheme and the Markov model developed for the EPC Gen-2 protocol in Chapter 5, we compare these two techniques in terms of the expected number of queries and the total amount of transmitted data required to identify all tags in an RFID system. Such a performance analysis is helpful for RFID system deployment and in designing new algorithms for improving the tag identification performance. Moreover, this chapter provides an analytical model for researchers in the field to easily compare their proposed protocols with the CDMA-based schemes as well as the standard EPC Gen-2 protocol.

The contributions of this chapter are as follows:

1. We study the CDMA-based tag identification scheme and model it as an absorbing Markov chain system.

2. Using this model, we derive the analytical formulae for the expected number of queries ($\overline{q}$) and the total transmitted data ($\overline{TD}$) needed to identify all tags in the system using the CDMA technique.

3. We compare the performance of the EPC Gen-2 protocol and the CDMA-based tag identification schemes and show that the EPC Gen-2 protocol outperforms the CDMA-based scheme in terms of the total transmitted data ($\overline{TD}$).

The rest of this chapter is organized as follows: In Section 6.2, we propose an absorbing Markov model for the CDMA-based tag identification schemes. We derive the analytical formulae for the expected number of queries and the total transmitted data required to identify all tags in the CDMA-based RFID systems. In Section 6.3, we compare the performance of the CDMA-based tag identification schemes and the standard EPC Gen-2

tag identification protocol in terms of the total number of required queries and the total transmitted data. The conclusion and further discussions are presented in Section 6.4.

6.2 CDMA-based Tag Identification

As discussed earlier, the CDMA technique has been widely suggested for the RFID systems recently. In traditional spread-spectrum (SS) systems such as CDMA systems, each user encodes its data using a spreading code which is orthogonal (or as close to orthogonal as possible) to the spreading codes of other users. This allows the successful decoding of data sent by two or more users simultaneously [61]. Using this idea, it has been suggested that several spreading codes are stored in each tag in an RFID system. Each spreading code consists of a predefined number of rectangular pulses, called the chips. Therefore, the lengths of a spreading code is defined by the number of its chips. Each tag randomly selects one of these codes to spread (encode) its ID, and then sends its coded ID to the reader. This technique has been shown in Fig. 6.1. Using the CDMA technique, multiple tags can be read simultaneously in each frame and thus the number of collisions is reduced. Although using the CDMA technique can reduce the number of collisions and increase the number of identified tags at each query, the assumption that it speeds-up the whole tag identification procedure may not necessarily be true and should be investigated more carefully.

6.2.1 Tag Identification Procedure

In order to use the CDMA technique, each bit of the tag ID should be first spread by the user specific code and then transmitted to the reader. This means that the length of the coded tag ID becomes longer after being encoded by the tag's spreading code. As an example, if the tags use spreading codes of length l in a CDMA-based RFID system, each

bit of the binary tag ID would be represented by a sequence of l binary chips. As a result, two different scenarios may happen. In the first scenario, the transmission rate should be increased to compensate for the increase in the number of chips (data) that should be transmitted for each tag ID. In the second scenario, the tag simply transmits all the chips of the spread tag ID one by one with the same transmission rate as the one recommended by the EPC Gen-2 standard. In other words, the transmission rate does not change in the second scenario. The first scenario does not seem to be a good option since the frequency band and the transmission rate in RFID systems have been standardized and most of the current RFID systems have been designed and operate based on the EPC Gen-2 standard. Moreover, changing the transmission rate would require significant changes in the hardware architecture of the RFID tags. In the second scenario, on the other hand, we do not need to significantly change the hardware architecture of RFID tags and the old system can still be used. The only modifications required are adding a cheap and small memory to each tag to store the spreading codes, and to update the readers in a way that they read a longer sequence of binary data and decode the tag IDs from the CDMA sequence.

As an example, in Fig. 6.1 it has been assumed that a tag whose ID is 01 needs to send its ID to the reader in a CDMA-based RFID system, and it randomly selects the 1010 spreading code. Therefore, the spread data that should be transmitted to the reader is 01011010. In the second scenario, the transmission rate of the tag is not changed for using the CDMA technique, so the time needed to transmit an information bit is the same as the time needed to transmit a chip. Therefore, assuming that the transmission rate of the tag is 1 bit per second and using the second scenario, it takes 8 seconds for the tag to transmit all the 8 chips to the reader. The received data (chips) is then multiplied by the spreading code in the reader and the 01 (ID) is detected.

Although the amount of transmitted data increases using the CDMA technique (both

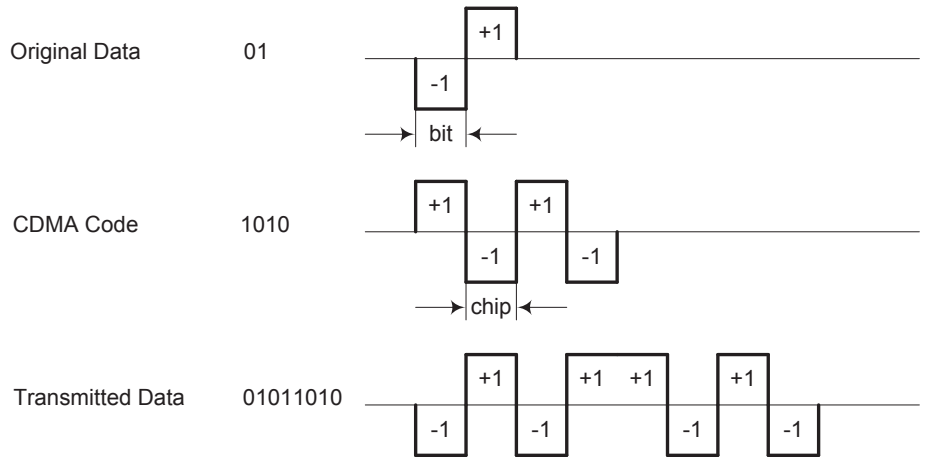

Figure 6.1: The CDMA technique, the bit and the chip concepts we used for RFID systems.

the first and the second scenarios), the number of collisions decreases for sure and more tag IDs are identified at each round of query compared to the ALOHA-based technique used by the EPC Gen-2 protocol. In other words, using the CDMA technique results in fewer queries but at each query more data should be transmitted by the tags. Therefore, we need to find (calculate) the expected number of queries and the total transmitted data for both the standard ALOHA-based and the CDMA-based tag identification protocols to be able to have a fair comparison between them.

6.2.2 Proposed Absorbing Markov Chain Model

As in the case of the EPC Gen-2 protocol in Chapter 5, we model the CDMA-based tag identification technique as an absorbing Markov chain. This model is shown in Fig. 6.2. For an RFID system with n tags, the proposed model has $n + 1$ states starting at state n on the left and ending at state 0. The number assigned to each state shows the number of tags in the system that have not been identified yet. We assume that d codes of length l are also used by the tags to encode their IDs. Using the CDMA technique, each tag chooses one of the d codes stored in its memory at random, encodes its ID and transmits

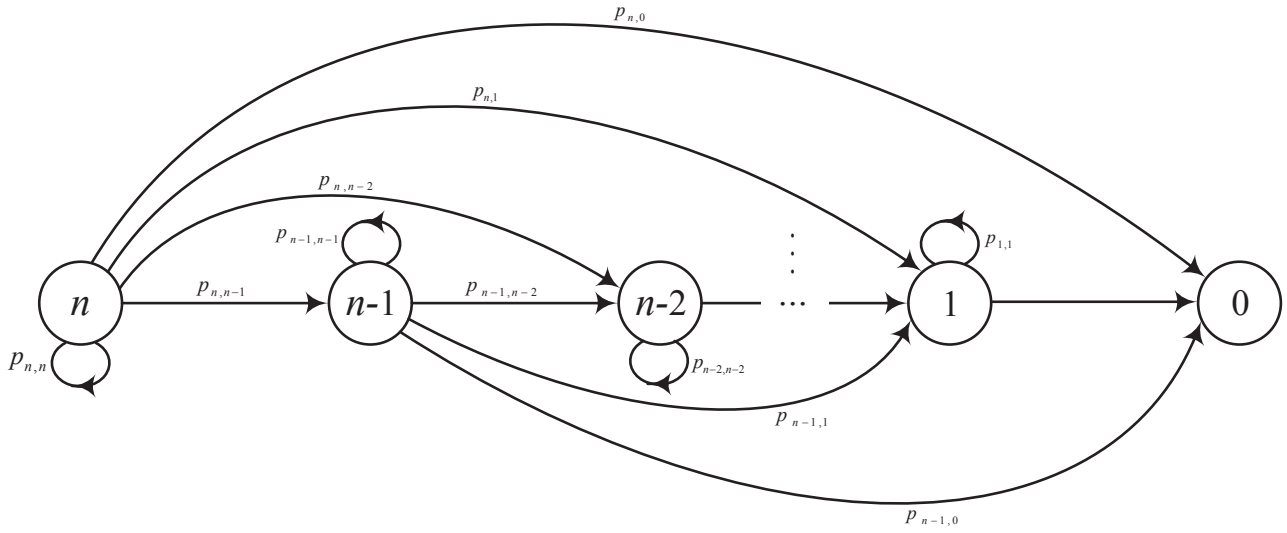

Figure 6.2: Our Proposed Markov chain model for the CDMA system.

the result to the reader. In the reader, all d codes are examined one by one to decode the information sent by the replying tags. In this tag identification technique, a tag is forced to be silent after it has been successfully identified by the reader. Using the above assumptions, two scenarios may happen. First, the tag chooses a spreading code which is not used by any other tag. As a result, the reader successfully decodes the ID sent by this tag. In the second scenario, two or more tags choose the same spreading code. As a result, a collision happens and the reader cannot read the information sent by the tags and identify their IDs.

In order to formulate the proposed Markov model, first we need to calculate the probability of jumping from state y to state z. In this model, $p_{y,z}$ means there were y tags in the system, and after being queried by the reader, $y - z$ tags were identified successfully while z tags remained unidentified in the system. In other words, $y - z$ spreading codes (out of the total d codes) were only chosen by $y-z$ separate tags, so the transmission of these $y-z$ tags was successful while the other $d-y+z$ spreading codes were chosen by more than one

tag. We can consider this problem as putting n balls (tags) in d baskets (spreading codes) and calculating the probability of having $y - z$ baskets occupied by one and only one tag. This is a well-known problem in the classical urn model and the probability is provided in [95]. Assuming that C baskets were chosen by more than one ball, E baskets were not chosen by any ball and S baskets were chosen by S balls (one ball in each basket), we have

$$d = E + S + C \ . \tag{6.1}$$

First, the probability of having E empty baskets is derived. This probability is denoted by $P_1(E, n, d)$ and is equal to

$$P_1(E, n, d) = \left(1 - \frac{E}{d}\right)^n, \qquad 0 \leq E \leq d \ . \tag{6.2}$$

In the next step, the probability of having S baskets each occupied by one ball only, conditional on having E empty baskets in the previous step is derived. This probability is denoted by $P_2(S\ , n\ ,\ d|\ E)$

$$\begin{aligned} P_2(S\ , n\ ,\ d|\ E) = & \binom{n}{S} \left(\frac{S}{d-E}\right)^S \left(1 - \frac{S}{d-E}\right)^{(n-S)} \\ & \times \left(\sum_{i=0}^{S} (-1)^i \binom{S}{i} \left(1 - \frac{i}{S}\right)^S\right), \\ & 0 \leq S \leq \min\{d - E, n\} \end{aligned} \tag{6.3}$$

where $\left(\frac{S}{d-E}\right)^S$ is the probability that S balls are assigned to the first S baskets in the total remaining $(d - E)$ baskets, $\left(1 - \frac{S}{d-E}\right)^{(n-S)}$ is the probability that the remaining $(n - S)$ balls are assigned to the remaining $(d - E - S)$ baskets, and the summation $\sum_{i=0}^{S} (-1)^i \binom{S}{i} \left(1 - \frac{i}{S}\right)^S$ is the probability that the mentioned S balls are assigned to S baskets, *with no basket remains empty* (in other words, each of the S baskets only accom-

modates one and only one of the S balls). The summation $\sum_{i=0}^{S}(-1)^i\binom{S}{i}\left(1-\frac{i}{S}\right)^S$ can be simplified as

$$\sum_{i=0}^{S}(-1)^i\binom{S}{i}\left(1-\frac{i}{S}\right)^S=\frac{S!}{S^S}\ . \tag{6.4}$$

Based on the above, $P_2(S\ ,n\ ,\ d|\ E)$ can be written as

$$\begin{aligned} P_2(S\ ,n\ ,\ d|\ E) &= \binom{n}{S}\left(\frac{S}{d-E}\right)^S \\ &\quad\times\left(1-\frac{S}{d-E}\right)^{(n-S)}\frac{S!}{S^S} \\ &= \binom{n}{S}\left(\frac{(d-E-S)^{(n-S)}}{(d-E)^n}\right)S!\ . \end{aligned} \tag{6.5}$$

Now, we need to calculate the probability of observing C baskets with more than one ball in each of them conditional on having E empty and S singly occupied baskets. For $P_3(C\ ,n\ ,\ d|\ E,S)$, it is not easy to calculate the probability of observing C conditional on E and S directly. Therefore, we define a class of acceptable events that represents different ways of distributing $(n-S)$ balls in C baskets such that each basket contains *at least* two balls. We define the number of these acceptable events as $r_{n-S}(C,2)$. We have

$$P_3(C\ ,n\ ,\ d|\ E,S)=\frac{r_{n-S}(C,2)}{C^{(n-S)}}\ , \tag{6.6}$$

in which $C^{(n-S)}$ is the total number of ways by which we can assign $(n-S)$ balls to the remaining C baskets. Now, the main problem is to determine $r_{n-S}(C,2)$. Riordan [96] suggested two closed form expressions for $r_\beta(\delta,\lambda)$ using the classical urn model in which β, δ and λ denote the number of balls, the number of baskets, and the minimum number of balls in each basket, respectively. The first closed form expression for $r_\beta(\delta,\lambda)$ is

$$r_\beta(\delta,\lambda)=\delta r_{\beta-1}(\delta,\lambda)+\delta\binom{\beta-1}{\lambda-1}r_{\beta-\lambda}(\delta-1,\lambda), \tag{6.7}$$

and the second one is

$$r_\alpha(\delta,\lambda) = \sum_{k=0}^{\delta}(-1)^k\binom{\delta}{k}\frac{\beta!}{(\lambda-1)!^k(\beta-\lambda k+k)!} \times r_{\beta-\lambda k+k}(\delta-k,\lambda-1). \tag{6.8}$$

Using Eq. (6.7) and (6.8), we can find the exact number of acceptable events in Eq. (6.6) by replacing β with $(n-S)$, δ with C and λ with 2 for our problem. The above recursive equations can be calculated in two different ways. In the first approach, we can only use Eq. (6.7) and combine it with three simple logical constraints, as stated below:

a) **if** $(\beta \neq 0)$ **and** $(\delta = 0)$, **then** $r_\beta(\delta,\lambda) = 0$;

b) **if** $(\beta < \delta\lambda)$, **then** $r_\beta(\delta,\lambda) = 0$;

c) **if** $(\delta = 1)$ **and** $(\beta \neq 0)$ **and** $(\beta \geq \delta\lambda)$, **then** $r_\beta(\delta,\lambda) = 1$.

Using this method, we can start from an initial point and find the exact value for $r_\beta(\delta,\lambda)$ recursively. As the second approach, we can simplify Eq. (6.8) by replacing λ with 2 and write

$$r_\alpha(\delta,2) = \sum_{k=0}^{\delta}(-1)^k\binom{\delta}{k}\frac{\beta!}{(\beta-k)!}r_{\beta-k}(\delta-k,1) \tag{6.9}$$

in which

$$r_{\beta-k}(\delta-k,1) = p_0(\beta-k,\delta-k)\ (\delta-k)^{(\beta-k)}\ , \tag{6.10}$$

and $p_0(\beta-k,\delta-k)$ is the probability that we have $(\beta-k)$ balls and $(\delta-k)$ baskets and all the baskets contain at least one ball. From [95], we have the mathematical expression for $p_0(\beta-k,\delta-k)$ as

$$p_0(\beta-k,\delta-k) = \sum_{v=0}^{\delta-k}(-1)^v\binom{\delta-k}{v}\left(1-\frac{v}{\delta-k}\right)^{(\beta-k)}. \tag{6.11}$$

By substituting Eq. (6.10) and (6.11) into (6.9), we get

$$r_{\beta}(\delta,2) = \sum_{k=0}^{\delta}\sum_{v=0}^{\delta-k}(-1)^{(k+v)}\binom{\delta}{k}\binom{\delta-k}{v} \times \frac{\beta!}{(\beta-k)!}(\delta-k-v)^{(\beta-k)} \ . \tag{6.12}$$

Based on the above, Eq. (6.6) can be written as

$$P_3(C\ ,n\ ,\ d|\ E,S) = \sum_{k=0}^{C}\sum_{v=0}^{C-k}(-1)^{(k+v)}\binom{C}{k}\binom{C-k}{v} \times \frac{(n-S)!}{(n-S-k)!}\frac{(C-k-v)^{(n-S-k)}}{C^{(n-S)}} \ . \tag{6.13}$$

Using Eq. (6.2), (6.5), (6.6) and (6.12) or (6.7), we can determine $P(E,S,C,n,d)$ as

$$P(E,S,C,n,d) = \left(\frac{d!}{E!\ S!\ C!}\right)\ P_1(E)\ P_2(S\ ,n\ ,d|\ E) \times P_3(C\ ,n\ ,\ d|\ E,S) \ . \tag{6.14}$$

In Eq. (6.14), $\left(\frac{d!}{E!\ S!\ C!}\right)$ is the number of ways by which the empty and singly occupied baskets and the ones containing more than one ball can be scrambled and mixed with each other and make a random structure of E, S and C baskets.

After deriving the analytical expression for $P(E,S,C,n,d)$, we use it to calculate the $p_{y,z}$ probabilities needed to complete the Markov model shown in Fig. 6.2. Using this Markov model and the technique we used for the EPC Gen-2 protocol in Chapter 5, we derive the accurate closed form expressions for the expected number of queries and the total transmitted data in the CDMA-based RFID systems.

6.2.3 Expected Number of Required Queries

As done in Chapter 5 Section 5.4.1, we arrange the order and indices of the states so that they can be divided into two separate groups, the transient states and the absorbing states. In Fig. 6.2, the first N circles (shown by N to 1) are the transient states, and the rightmost circle (shown by 0) is the absorbing state. Now, the transition matrix of the Markov system in Fig. 6.2 can be written as below

$$\mathbf{P} = \begin{array}{c} \\ \text{Tr.} \\ \\ \text{Abs.} \end{array} \begin{array}{c} \begin{array}{cc} \text{Tr.} & \text{Abs.} \end{array} \\ \left[\begin{array}{c|c} \mathbf{G} & \mathbf{H} \\ \hline \mathbf{0} & \mathbf{I} \end{array}\right] \end{array}$$

where $\mathbf{P}$ is the transition matrix, $p_{i,j}$ denotes the probability of transition from state i to state j, $\mathbf{G}$ is the matrix of transient states, $\mathbf{H}$ is the matrix of the absorbing states, $\mathbf{0}$ is the zero matrix and $\mathbf{I}$ is the identity matrix. From the Markov chain theorem, we know that the probability of the system being in the transient state j after x jumps and having started from the transient state i is given by $g_{i,j}^{x}$, where $g_{i,j}^{x}$ is the i,jth component of matrix $\mathbf{G}^{x}$. The following specifications of the $\mathbf{G}$ matrix given by *Lemma 1* and *Lemma 2* are critical in deriving the analytical expressions for the expected number of queries and the total transmitted data.

Lemma 1: If the number of jumps (transitions) tends to infinity, then $\lim_{x\to\infty} \mathbf{G}^{x} = 0$.

Lemma 2: In the proposed Markov model, $(\mathbf{I} - \mathbf{G})^{-1}$ always exists, where $\mathbf{I}$ is the corresponding identity matrix of the same size as $\mathbf{G}$.

The proofs of the above two lemmas are exactly the same as Chapter 5. We use these two lemmas to derive a closed form expression for the expected number of queries and the

total transmitted data. Using the second lemma, we define a matrix $\mathbf{M}$ as

$$\mathbf{M} = (\mathbf{I} - \mathbf{G})^{-1} . \tag{6.15}$$

We also have

$$\mathbf{I} - \mathbf{G}^{x+1} = (\mathbf{I} - \mathbf{G}) \times (\mathbf{I} + \mathbf{G} + \mathbf{G}^2 + \mathbf{G}^3 + ... + \mathbf{G}^x) . \tag{6.16}$$

Multiplying Eq. (6.16) by $\mathbf{M}$, we get

$$\mathbf{M} \times (\mathbf{I} - \mathbf{G}^{x+1}) = (\mathbf{I} - \mathbf{G})^{-1} \times (\mathbf{I} - \mathbf{G}) \times (\mathbf{I} + \mathbf{G} + \mathbf{G}^2 + \mathbf{G}^3 + ... + \mathbf{G}^x) . \tag{6.17}$$

From the first lemma we have $\lim_{x\to\infty} \mathbf{G}^x = 0$, so by letting x tend to infinity we get

$$\mathbf{M} = (\mathbf{I} + \mathbf{G} + \mathbf{G}^2 + \mathbf{G}^3 + ...) \tag{6.18}$$

or equivalently,

$$m_{i,j} = g_{i,j}^0 + g_{i,j}^1 + g_{i,j}^2 + ... \tag{6.19}$$

Now let i and j be two transient states, and $\alpha_{i,j}(k)$ be a random variable which equals 1 if the absorbing Markov chain of Fig. 6.2 reaches state j after exactly k jumps and starting from state i, and $\alpha_{i,j}(k)$ equals 0 otherwise. According to matrix $\mathbf{G}$ we have

$$Pr(\alpha_{i,j}(k) = 1) = g_{i,j}^k \tag{6.20}$$

$$Pr(\alpha_{i,j}(k) = 0) = 1 - g_{i,j}^k \tag{6.21}$$

where $g_{i,j}^k$ is the i,jth entry of $\mathbf{G}^k$. The expected number of times that the absorbing Markov chain is in state j in the first k steps, given that it starts at state i is

$$\begin{aligned} & E\{\alpha_{i,j}(0) + \alpha_{i,j}(1) + \alpha_{i,j}(2) + ... + \alpha_{i,j}(k)\} \\ = \;& E\{\alpha_{i,j}(0)\} + E\{\alpha_{i,j}(1)\} + ... + E\{\alpha_{i,j}(k)\} \\ = \;& g_{i,j}^0 + g_{i,j}^1 + g_{i,j}^2 + ... + g_{i,j}^k \; . \end{aligned} \tag{6.22}$$

Letting k tend to infinity, we get

$$\begin{aligned} & E\{\alpha_{i,j}(0) + \alpha_{i,j}(1) + \alpha_{i,j}(2) + ...\} \\ = \;& g_{i,j}^0 + g_{i,j}^1 + g_{i,j}^2 + ... \; . \end{aligned} \tag{6.23}$$

Finally from Eq. (6.19) and (6.23), we have

$$E\{\alpha_{i,j}(0) + \alpha_{i,j}(1) + \alpha_{i,j}(2) + ...\} = m_{i,j} \tag{6.24}$$

where $m_{i,j}$ is the i,jth entry of matrix $\mathbf{M}$ defined in Eq. (6.15). Based on the above, if a CDMA-based tag identification protocol starts from state i, the expected number of times that it visits state j before all the tags in the system are identified can be calculated from Eq. (6.24). We know that the CDMA-based protocol always starts from state N ($i = N$). Knowing this fact and using the Markov model shown in Fig. 6.2, we can simply conclude that the expected number of queries in the CDMA-based protocol is calculated by adding all entries of the Nth row of the $\mathbf{M}$ matrix, i.e.,

$$\bar{q} = \sum_{j=1}^{N} m_{N,j} \tag{6.25}$$

where $\bar{q}$ is the average number of queries required to identify all of the N tags in the system. Using the above formulation, there is no need to run multiple simulations and average them to obtain the number of queries needed to identify all tags in the system, instead, we can simply use Eq. (6.25) and calculate $\bar{q}$ directly.

6.2.4 Expected Number of Transmitted Chips

After deriving the closed form expression of the expected number of queries, we need to derive the closed form expression of the aggregate number of chips that are sent by the tags, before they are successfully identified by the reader. According to [3], we assume that each tag ID is 96 bits long. Assuming that each tag selects a spreading code of length l out of the total d codes at random, the total number of transmitted chips in the CDMA-based system is

$$\overline{TC} = \bar{q} \times l \times 96 \tag{6.26}$$

where $\overline{TC}$ shows the total expected number of transmitted chips, $\bar{q}$ is the expected number of queries calculated from Eq. (6.25), and l is the length of spreading codes used by tags.

6.3 Performance Comparison

This section presents the results of the simulation experiments we carried to evaluate the performance of the CDMA-based tag identification schemes and to compare it with the standard EPC Gen-2 protocol. To compare these schemes, we use the Markov model proposed for the EPC Gen-2 protocol in Chapter 5 as well as the one we developed in this chapter for the CDMA-based tag identification procedure. Using these analytical models, we calculate the expected number of queries required to identify all the tags in

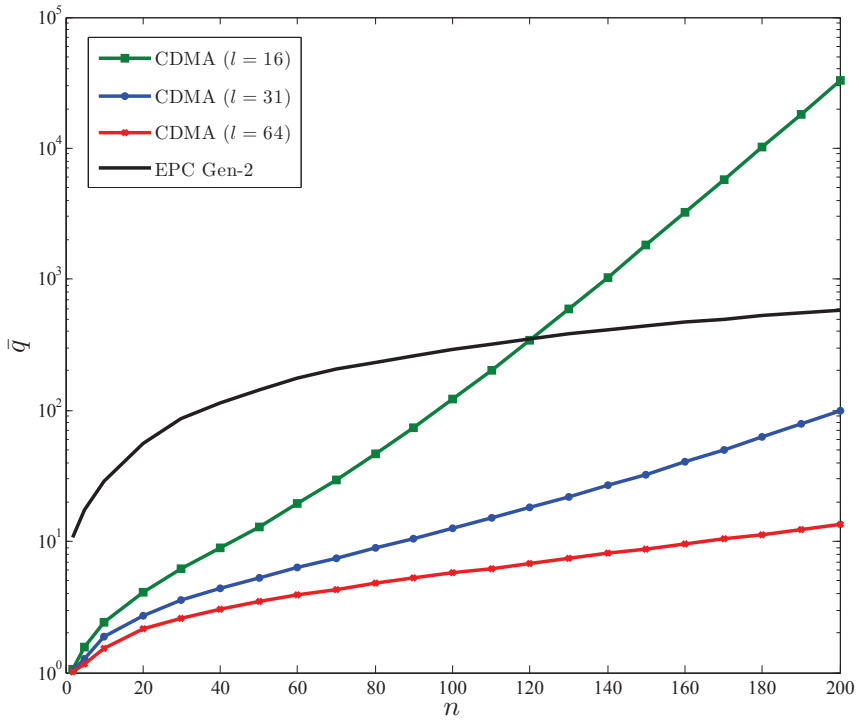

Figure 6.3: The expected number of required queries $\bar{q}$ for detecting all tags vs. the number of tags in the system for both the EPC protocol ($c = 0.2$) and the CDMA-based tag identification scheme ($l = 16, 31, 64$).

the system for both the EPC Gen-2 and the CDMA schemes. We also use these analytical models to calculate and compare the total number of bits transmitted using the EPC Gen-2 protocol and the total number of chips transmitted using the CDMA-based tag identification scheme. All simulations have been performed in the MATLAB environment.

We first consider an RFID system which operates based on the EPC Gen-2 protocol. We initialize c to 0.2, vary n (the number of tags in the system) between 0 and 200, and calculate the number of queries needed to identify all tags in the RFID system. Then, we consider a CDMA-based RFID system and calculate the number of queries required when it uses spreading codes of length 16, 31 and 64 chips, respectively. Performance comparison of the two systems (in terms of the expected number of queries) is shown in Fig. 6.3. As expected, the CDMA-based scheme outperforms the EPC Gen-2 protocol in terms of the

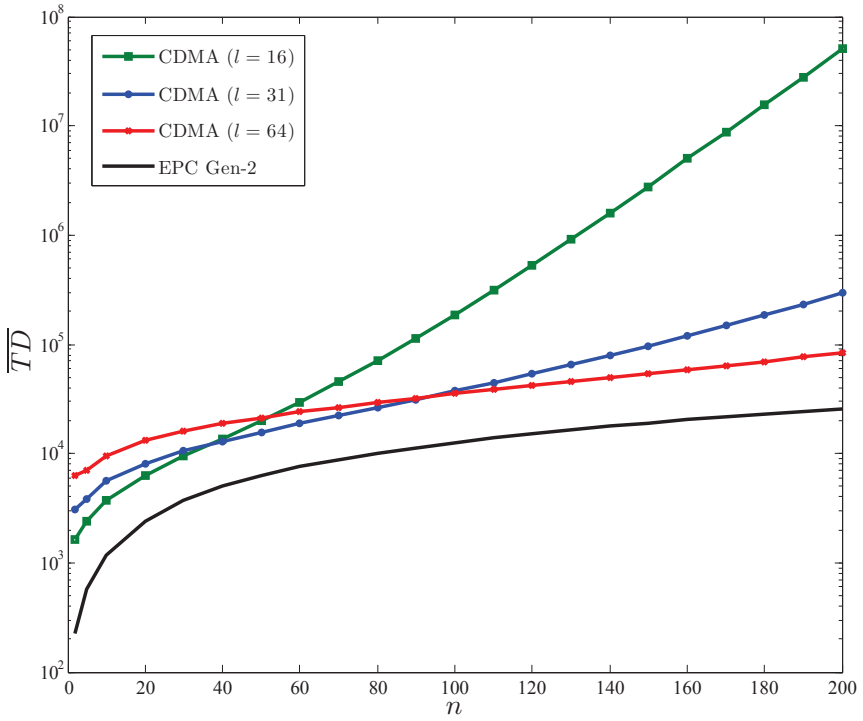

Figure 6.4: The total transmitted data $\overline{TD}$ for detecting all tags vs. the number of tags in the system for both the EPC protocol ($c = 0.2$) and the CDMA-based tag identification scheme ($\overline{TD}_{EPC} = \overline{TB}$, $\overline{TD}_{CDMA} = \overline{TC}$, and $l = 16, 31, 64$).

number of required queries. It is obvious that the more spreading codes the tags can choose from, the less chance there is for collisions and therefore, fewer queries are needed.

Although the expected number of required queries in the CDMA-based tag identification schemes is fewer compared to the EPC Gen-2 protocol, it does not necessarily mean that the CDMA schemes can identify the tags more efficiently. As mentioned in Section 6.1, the total transmitted data is another factor (and probably the more important one) to judge the efficiency of the CDMA-based scheme and the EPC Gen-2 protocol. Assuming that each chip (bit) needs t seconds to be transmitted, the total time needed to identify all tags in the system is $t \times \overline{TD}$. Therefore, it is a plausible assumption that the total time needed to identify all tags in the system is a function (multiple) of the $\overline{TD}$ calculated in Chapter 5

and Chapter 6. It should be noted that for the EPC Gen-2 protocol, $\overline{TD}_{EPC} = \overline{TB}$ and it is calculated using Eq. (5.34), and for the CDMA systems, $\overline{TD}_{CDMA} = \overline{TC}$ and it is calculated using Eq. (6.26). Fig. 6.4 shows the total transmitted data for the EPC Gen-2 protocol and the CDMA-based tag identification technique, assuming that the parameter c is set to 0.2 [3] and the CDMA scheme uses the spreading codes of length 16, 31 and 64. Interestingly, it can be observed from the figure that the standard EPC Gen-2 protocol outperforms the CDMA-based scheme in terms of the total transmitted data (and equivalently the total time needed to identify all tags). In other words, for all values of n, the EPC Gen-2 protocol detects all tags in the system using fewer number of transmitted bits compared to the number of transmitted chips in the CDMA-based tag identification scheme.

As explained in [3], the value of c in the EPC Gen-2 protocol can be chosen from 0.1 to 0.5 by the designer based on the system requirements and the applications. Therefore, we set the value of c to 0.4 and repeated the above procedure again. The results are shown in Fig. 6.5 and 6.6. The expected number of queries is shown in Fig. 6.5 for both the EPC Gen-2 protocol and the CDMA-based tag identification scheme. As expected, the CDMA scheme needs fewer queries to identify all the tags in the system. It is obvious that the more spreading codes the tags have to choose from, the fewer is the number of collisions and therefore, the fewer queries are needed. However, Fig. 6.6 reveals that the EPC Gen-2 protocol still outperforms the CDMA-based tag identification scheme in terms of the transmitted data needed to identify all tags in the system.

6.4 Summary

In this chapter, we studied the CDMA-based tag identification protocol and modeled it as an absorbing Markov chain. Then, we formulated the model and derived the closed

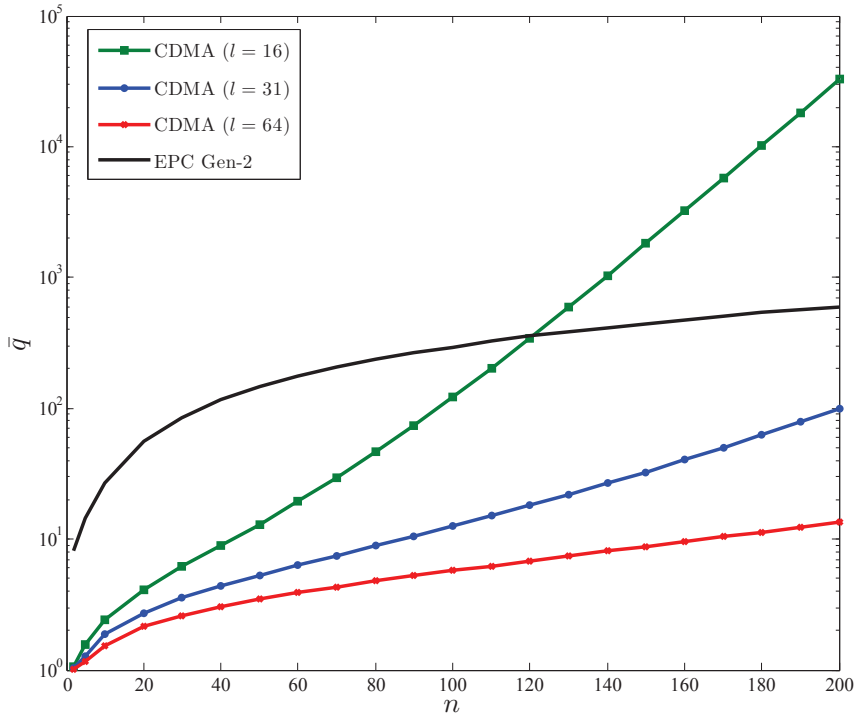

Figure 6.5: The total transmitted data $\overline{TD}$ for detecting all tags vs. the number of tags in the system for both the EPC protocol ($c = 0.4$) and the CDMA-based tag identification scheme ($l = 16, 31, 64$).

form analytical expressions for the expected number of queries and the total transmitted data needed to identify all tags in the system. We also used the absorbing Markov model proposed in Chapter 5 for the EPC Gen-2 protocol. Using these two analytical models, the CDMA-based tag identification procedure was compared with the standard EPC Gen-2 protocol in terms of the total expected number of queries and the total transmitted data required to identify all tags in the RFID systems.

It was shown that the expected number of queries decreases if the CDMA technique is used for the tag identification purpose instead of the EPC Gen-2 protocol. This is because the number of collisions decreases when the CDMA technique is used. It is obvious that the more spreading codes used by the tags, the less chance for collisions and the fewer the expected number of queries. However, the story is different for the amount

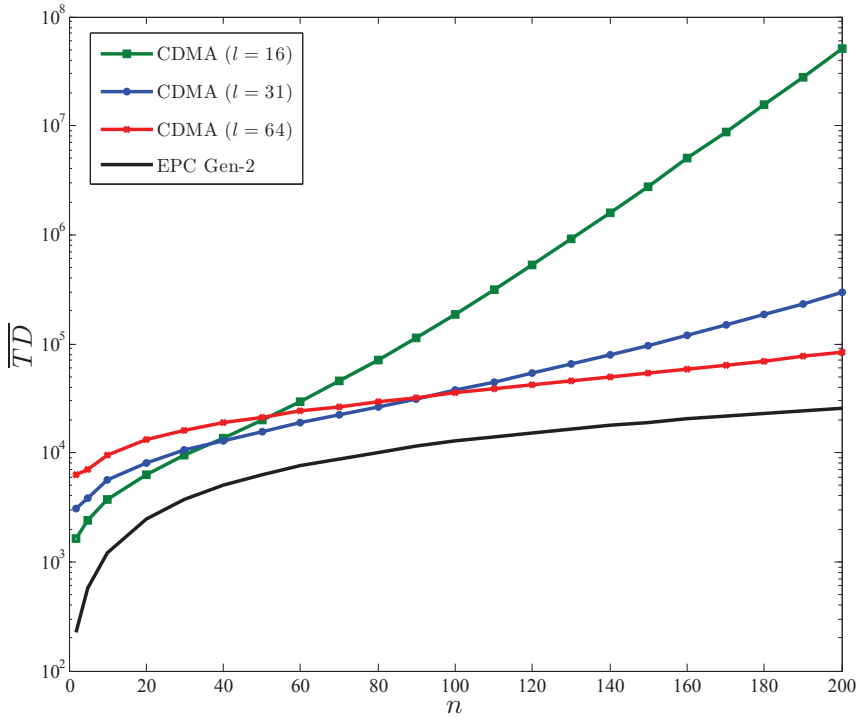

Figure 6.6: The total transmitted data $\overline{TD}$ for detecting all tags vs. the number of tags in the system for both the EPC protocol ($c = 0.4$) and the CDMA-based tag identification scheme ($\overline{TD}_{EPC} = \overline{TB}$, $\overline{TD}_{CDMA} = \overline{TC}$, and $l = 16, 31, 64$).

of data that should be transmitted, and for the time needed to identify all tags in the system. Our study revealed that the EPC Gen-2 protocol outperforms the CDMA-based tag identification scheme in terms of the total transmitted data (and of course the total time needed) to identify all the tags in the RFID systems. Reducing the total transmitted data (and consequently reducing the required tag identification time) was the main idea behind proposing the CDMA technique for RFID applications. However, this study revealed that the CDMA technique cannot beat the EPC Gen-2 protocol in terms of the total transmitted data and the required time. Therefore, changing the current standard protocol and modifying the hardware architecture of the current passive RFID tags (to make them capable of performing CDMA transmission) may not be a better solution. It should be noted that we did not design our analytical model based on the first or second CDMA

scenarios mentioned in Section 6.2.1. Therefore, the proposed analytical model and the performance evaluation results are valid for both the first and second scenarios.

It should also be noted that in the proposed analytical model, it was assumed that we have complete synchronization between the reader and all the tags. This means that all the tags transmit their IDs concurrently and in complete synchronization with the reader. It was also assumed that the spreading codes used by the tags are orthogonal codes (like Walsh codes) with zero cross-correlation [77, 121]. In reality, however, complete synchronization is a hard condition to achieve. Therefore, it has been suggested to use PN sequences like Gold and Kasami codes instead of orthogonal codes [61]. PN codes have better cross-correlation specifications compared to orthogonal codes, and therefore, can better tolerate poor synchronization situations. However, more queries would be needed if PN codes are used instead of the orthogonal codes, due to the autocorrelation characteristics of the PN codes. In other words, we modeled and formulated the CDMA-based tag identification scheme under ideal conditions (assuming complete synchronization and using orthogonal codes). The expected number of queries and the total transmitted data would increase if any of the two mentioned conditions is not satisfied. Fig. 6.3 to Fig. 6.6 show the best possible (the ideal) performance of the CDMA-based tag identification system. This work can be extended by considering the synchronization problem and the autocorrelation issue of the PN codes in our Markov model as a future work.

In this chapter, the proposed Markov model was used to formulate the CDMA-based tag identification scheme and to calculate the expected number of queries and the total transmitted data. This analytical model, however, can be used for many other purposes such as estimating the number of tags in an area of interest or for improving the performance of RFID systems.

Chapter 7

Conclusions and Future Work

In this chapter, we conclude the thesis by summarizing our results and highlighting the contributions of this dissertation. We also suggest several topics for further research.

7.1 Research Contributions

The four analytical models we developed for RFID systems are the most important contributions of this thesis. We developed an analytical model for RFID systems that operate based on the binary tree walking technique. We also developed an analytical model for RFID systems that operate based on the ALOHA technique. To the best of our knowledge, the probabilistic analysis of the binary tree walking-based and ALOHA-based RFID systems has been accomplished in this thesis for the first time. In this thesis, we modeled the tag identification process of the EPC Class-1 Gen-2 UHF standard as an absorbing Markov chain, and developed an accurate analytical model for it. The tag identification process used by the EPC Class-1 Gen-2 UHF standard is exactly the same as the one used by the EPC Class-1 HF standard. Therefore, the analytical model we developed for the EPC Class-1 Gen-2 UHF standard can be directly applied to the EPC Class-1 HF standard. Prior to our Markov model, there was only one other analytical model for the EPC Class-1 Gen-2 standard [1]. We also modeled the CDMA-based RFID systems as an absorbing Markov chain, and developed an accurate analytical model for these systems. To the best of our knowledge, the use of a Markov model for the CDMA tag identification technique

has been proposed in this thesis for the first time. The four analytical models developed in this thesis can be used in multiple areas and for different purposes, as explained in Chapter 1.

In this thesis, we considered two challenging areas in RFID systems. First, we studied the security and privacy of RFID systems in Chapters 2 and 3, and proposed several solutions to improve the security and privacy of RFID systems. In the second step, we focused on the efficiency of the tag singulation schemes in RFID systems. We performed analytical modeling and performance analysis of the tag singulation schemes in Chapters 4, 5 and 6. Below is the detailed list of our contributions in each chapter.

- In Chapter 2, we first studied the blocking attack in RFID systems that operate based on the binary tree walking tag singulation mechanism, and developed an analytical model for this attack against the binary tree walking-based RFID systems. Using the analytical model developed, we proposed a probabilistic blocker tag detection algorithm (P-BTD) to detect the presence of an attacker in this type of RFID systems. Then, we focused on RFID systems that operate based on the ALOHA tag singulation mechanism, and developed an analytical model for the blocking attack against the ALOHA-based RFID systems. Using this analytical model, we proposed a probabilistic blocker tag detection algorithm (P-BTD) to detect the presence of an attacker in this type of RFID systems. Simulation results revealed that the proposed P-BTD algorithms expedite the blocker detection process in both the binary tree walking and ALOHA-based RFID systems.

- In Chapter 3, we investigated the security and privacy issues of the standard EPC Gen-2 protocol, and studied the use of light-weight cryptography for increasing the security and privacy in RFID systems. We performed the security analysis of several light-weight RFID protocols recently proposed for RFID applications, and showed

their vulnerabilities. Using this security analysis, we proposed a new light-weight authentication protocol which improves the level of security and privacy in RFID systems. In designing the new light-weight protocol, the hardware limitation of passive RFID tags was taken into consideration.

- In Chapter 4, we used the analytical model we derived in Chapter 3 to develop a probabilistic tag estimation scheme. First, it was shown that the tag estimation method proposed in [2] is incorrect. Then, using the probabilistic model derived in Chapter 3, we modified the model in [2] and proposed a new probabilistic tag estimation scheme for ALOHA-based RFID systems. In the proposed scheme, the reader estimates the number of RFID tags in the system after each interrogation based on *a posteriori* probability and uses this estimated number to determine the number of required time slots for the next interrogation.

- In Chapter 5, we studied the tag singulation mechanism in the EPC Gen-2 protocol and modeled it as an absorbing Markov chain. We formulated the proposed model and derived the expected number of queries required by the EPC Gen-2 protocol to identify all RFID tags in the system. We also derived the expected number of transmitted bits for the EPC Gen-2 protocol. These formulae allow us to provide a measure of the speed of the EPC Gen-2 protocol in identifying all tags in the system and the amount of data that should be transferred during this process.

- In Chapter 6, we focused on the tag singulation process in CDMA-based RFID systems. We modeled the CDMA-based RFID systems as an absorbing Markov chain, and derived the closed form analytical expression for the average number of queries required and the total transmitted data needed to identify all tags in the CDMA-based RFID systems. Taking advantage of the Markov model proposed in

Chapter 6 for the CDMA-based RFID systems and the one we developed for the EPC Gen-2 protocol in Chapter 5, the two tag singulation schemes were compared. It was shown that the EPC Gen-2 protocol outperforms the CDMA-based scheme in terms of the total transmitted data and the average time needed to identify all tags in the system.

7.2 Suggestions for Future Work

In the following, we consider several interesting possibilities for extension of the current work.

1. **Finding an Analytical Model for the Probability of Error in the Proposed P-BTD Algorithms.** In Chapter 2, we determined the probability of error for binary tree walking and ALOHA-based P-BTD algorithms using simulations. However, a better way is to use an analytical model to find the closed form expression of the probability of error. This is not a straightforward task, but it is a worthwhile study as it will enable us to perform the sensitivity analysis and determine the effect of using inaccurate values of N, F and p on the final performance of the proposed P-BTD algorithms. Moreover, the performance of the proposed P-BTD algorithms can be improved by modifying the decision criterion we used in Fig. 2.3 and Fig. 2.4.

2. **Extending the P-BTD Algorithm for the EPC Gen-2 Protocol.** We developed two P-BTD algorithms for detecting the presence of blocker tags in RFID systems that operate based on the binary tree walking or ALOHA mechanisms. However, it seems that the tag singulation mechanism proposed by the EPC Gen-2 protocol is dominating the binary tree walking and the ALOHA mechanisms in recent years. On the other hand and to the best of our knowledge, no solution has been

proposed so far for detecting the presence of blocker tags in RFID systems which use the EPC Gen-2 protocol. We have developed an absorbing Markov model for the EPC Gen-2 protocol in Chapter 5. This absorbing Markov model can be used along with the probabilistic blocker tag detection approach we used in Chapter 2 to provide a P-BTD algorithm for RFID systems that operate based on the EPC Gen-2 protocol.

3. **Reducing the Security Issues of RFID-based e-Passports.** In 2006, the US Department of State started embedding RFID chips in US passports to increase their security. Some European countries such as Germany and the Netherlands as well as some Asian countries like Malaysia also started issuing RFID embedded e-passports [24]. Starting on July 1, 2013, all newly issued Canadian passports will be e-Passports [122]. Although using the e-passports can make it harder for unauthorized persons to forge them and expedite the check-in process at airports, it can add serious threats and put the security, personal information and even the life of an e-passport holder into great risks [9, 24, 25]. The security of RFID-based e-passports has been a great concern for many countries and this is considered as an open problem today.

4. **Improving the Q-Algorithm Using Probabilistic Tag Estimation.** In Chapter 4, we introduced a new probabilistic method to estimate the number of tags in ALOHA-based RFID systems. We also developed an analytical model for the Q-algorithm and the tag singulation process of the EPC Gen-2 protocol in Chapter 5. These two techniques can be combined to provide a more efficient tag singulation process for RFID systems. In the traditional Q-algorithm used by the EPC Gen-2 protocol, the values of Q_{fp} are changed heuristically based on the responses the reader had received from the tags during its previous query. We can design a more advanced Q-algorithm which uses a probabilistic tag estimation method (similar to

the one proposed in Chapter 4) to first estimate the number of tags in the system and then change the value of Q_{fp} for the next query accordingly. This technique adds some computational costs to the system, however, these computational costs are added to the reader only, and not to the tags. In return, the tag singulation efficiency will increase using the advanced Q-algorithm.

5. **Synchronization and Orthogonality Issues in CDMA-based RFID Systems.** In the analytical model proposed for CDMA-based RFID systems in Chapter 6, it was assumed that we have complete synchronization between the reader and all the tags. This means that all the tags transmit their chips concurrently and in complete synchronization with the reader. It was also assumed that the spreading codes used by the tags are orthogonal codes (like Walsh codes) with zero cross-correlation [77, 121]. In reality, however, complete synchronization is a hard condition to achieve. Therefore, it has been suggested to use PN sequences like Gold and Kasami codes instead of orthogonal codes [61]. PN codes have better cross-correlation specifications compared to orthogonal codes, and therefore, can better tolerate poor synchronization situations. However, the autocorrelation of the PN codes is not as good as the orthogonal codes, therefore, more queries would be needed if PN codes are used instead of the orthogonal codes. We modeled and formulated the CDMA-based tag identification scheme under ideal conditions (assuming complete synchronization and using orthogonal codes). The expected number of queries and the total transmitted data would increase for sure if any of the two mentioned conditions is not satisfied. This work can be extended by considering the synchronization problem and the autocorrelation issue of the PN codes in our Markov model.

Bibliography

[1] C. Wang, M. Daneshmand, K. Sohrabi, and B. Li, "Performance analysis of RFID generation-2 protocol," *IEEE Trans. on Wireless Communications*, vol. 8, no. 5, pp. 2592–2601, May 2009.

[2] W.-T. Chen, "An accurate tag estimate method for improving the performance of an RFID anticollision algorithm based on dynamic frame length ALOHA," *IEEE Trans. on Automation Science and Engineering*, vol. 6, no. 1, pp. 9–15, Jan. 2009.

[3] EPCglobal, "EPC Radio-Frequency Identity Protocols: Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz Version 1.2," Oct. 2008. [Online]. Available: http://www.epcglobalinc.org/standards/uhfc1g2

[4] H. M. Sun and W. C. Ting, "A Gen2-based RFID authentication protocol for security and privacy," *IEEE Trans. on Mobile Computing*, vol. 8, no. 8, pp. 1052–1062, Aug. 2009.

[5] D. Henrici and P. Müller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," in *Proc. of IEEE PERCOM'04*, Orlando, FL, Mar. 2004.

[6] T. L. Lim, T. Li, and T. Gu, "Secure RFID identification and authentication with triggered hash chain variants," in *Proc. of IEEE ICPADS'08*, Melbourne, Australia, Dec. 2008.

[7] C. C. Tan, B. Sheng, and Q. Li, "Secure and serverless RFID authentication and search protocols," *IEEE Trans. on Wireless Communications*, vol. 7, no. 4, pp. 1400–1407, Apr. 2008.

[8] S. Ahson and M. Ilyas, *RFID Handbook: Applications, Technology, Security, and Privacy*. CRC Press, 2008.

[9] M. Meingast, J. King, and D. K. Mulligan, "Embedded RFID and everyday things: A case study of the security and privacy risks of the U.S. E-passports," in *Proc. of IEEE Int'l Conf. on RFID*, Grapevine, TX, Mar. 2007.

[10] V. Shah-Mansouri and V. W. Wong, "Cardinality estimation in RFID systems with multiple readers," *IEEE Trans. on Wireless Communications*, vol. 10, no. 5, pp. 1458–1469, May 2011.

[11] A. Cangialosi, J. E. Monaly, and C. S. Yang, "Leveraging RFID in hospitals: Patient life cycle and mobility perspectives," *IEEE Communications Magazine*, vol. 45, no. 9, pp. 18–23, Sept. 2007.

[12] A. Juels, "RFID security and privacy: A research survey," *IEEE J. on Selected Areas in Communication*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[13] J. Banks, M. Pachano, L. Thompson, and D. Hanny, *RFID Applied*. John Wiley, 2007.

[14] S. Shepard, *RFID: Radio Frequency Identification*. McGraw-Hill, 2005.

[15] D. Ma and A. K. Prasad, "A context-aware approach for enhanced security and privacy in RFID electronic toll collection systems," in *Proc. of ICCCN*, Hawaii, HI, Aug. 2011.

[16] X. Guangxian, "The research and application of RFID technologies in highways electronic toll collection system," in *Proc. of WiCOM*, Dalian, China, Oct. 2008.

[17] [Online]. Available: http://www.gs1.org/gsmp/kc/epcglobal

[18] J. Ayoade, "Roadmap to solving security and privacy concerns in RFID systems," *Computer Law and Security Report*, vol. 23, pp. 555–561, Sept. 2007.

[19] M. Langheinrich, "A survey of RFID privacy approaches," *Personal and Ubiquitous Computing*, vol. 13, pp. 413–421, Aug. 2009.

[20] E. Vahedi, V. Shah-Mansouri, V. Wong, I. F. Blake, and R. K. Ward, "Probabilistic analysis of blocking attack in RFID systems," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 3, pp. 803–817, Sept. 2011.

[21] D. Molnar and D. Wagner, "Privacy and security in library RFID: issues, practices, and architectures," in *Proc. of Computer and Communications Security Conf.*, Washington, DC, Oct. 2004.

[22] A. Juels and R. Pappu, "Squealing Euros: Privacy protection in RFID-enabled banknotes," in *Proc. of Financial Cryptography Conf.*, Guadeloupe, Jan. 2003.

[23] Y. Xiao, X. Shen, B. Sun, and L. Cai, "Security and privacy in RFID and applications in telemedicine," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 64–72, Apr. 2006.

[24] A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in e-passports," in *Proc. of Int'l Conf. on Security and Privacy for Emerging Areas in Communications Networks*, Athens, Greece, Sept. 2005.

[25] J. H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, and R. W. Schreur, "Crossing borders: Security and privacy issues of the European e-passport," in *Proc. of Int'l Workshop on Security*, Kyoto, Japan, Oct. 2006.

[26] R. C. W. Phan, "Cryptanalysis of a new Ultra-lightweight RFID authentication protocol-SASI," *IEEE Trans. on Dependable and Secure Computing*, vol. 6, no. 1, pp. 316–320, Mar. 2009.

[27] H. Liu and H. Ning, "Zero-knowledge authentication protocol based on alternative mode in RFID systems," *IEEE Sensors Journal*, vol. 11, no. 12, pp. 3235–3245, Dec. 2011.

[28] D. Maimut and K. Ouafi, "Light-weight cryptography for RFID tags," *IEEE Security and Privacy*, vol. 10, no. 2, pp. 76–79, Apr. 2012.

[29] E. Blass, A. Kurmus, R. Molva, G. Noubir, and A. Shikfa, "The f_f-family of protocols for RFID-privacy and authentication," *IEEE Trans. on Dependable and Secure Computing*, vol. 8, no. 3, pp. 466–480, June 2011.

[30] P. Rizomiliotis, E. Rekleitis, and S. Gritzalis, "Security analysis of the Song-Mitchell authentication protocol for low cost RFID tags," *IEEE Commun. Letters*, vol. 13, no. 4, pp. 274–276, Apr. 2009.

[31] H. M. Sun, W. C. Ting, and K. H. Wang, "On the security of the Chien's ultralightweight RFID authentication protocol," *IEEE Trans. on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1–3, July 2009.

[32] S. Piramuthu, "Lightweight cryptographic authentication in passive RFID-tagged systems," *IEEE Trans. on Systems, Man, and Cybernetics*, vol. 38, no. 3, pp. 360–376, May 2008.

[33] B. Calmels, S. Canard, M. Girault, and H. Sibert, "Low cost cryptography for privacy in RFID systems," in *Proc. of Int'l Conf. on Smart Card Research and Advanced Application*, Tarragona, Spain, Apr. 2006.

[34] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *Proc. of Int'l Conf. on Security and Privacy for Emerging Areas in Communications Networks*, Athens, Greece, Sept. 2005.

[35] J. Wu and D. R. Stinson, "How to improve security and reduce hardware demands of the WIPR RFID protocol," in *Proc. of IEEE Int'l Conf. on RFID*, Orlando, FL, Apr. 2009.

[36] H. Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," *IEEE Trans. on Dependable and Secure Computing*, vol. 4, no. 4, pp. 337–340, Dec. 2007.

[37] T. Cao, E. Bertino, and H. Lei, "Security analysis of the SASI protocol," *IEEE Trans. on Dependable and Secure Computing*, vol. 6, no. 1, pp. 73–77, Mar. 2009.

[38] S. Dolev, M. Kopeetsky, and A. Shamir, "RFID authentication, efficient proactive information security within computational security," *Theory of Computing Systems*, vol. 48, no. 1, pp. 132–149, Jan. 2011.

[39] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede, "Elliptic curve-based security processor for RFID," *IEEE Trans. on Computers*, vol. 57, no. 11, pp. 1514–1527, Nov. 2008.

[40] F. Furbass and J. Wolkerstorfer, "ECC processor with low die size for RFID applications," in *Proc. of IEEE Int'l Symposium on Circuits and Systems*, New Orleans, LA, May 2007.

[41] S. I. Ahmed, F. Rahman, and M. E. Hoque, "ERAP: ECC-based RFID authentication protocol," in *Proc. of 12th IEEE Int'l Workshop on Future Trends of Distributed Computing Systems*, Kunming, China, Oct. 2008.

[42] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "Public key cryptography for RFID tags," in *Proc. of 5th IEEE Int'l Conf. on Pervasive Computing and Communications Workshop*, White Plains, NY, Mar. 2007.

[43] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in *Proc. of Int'l Workshop on Cryptographic Hardware and Embedded Systems*, Cambridge, MA, Aug. 2004.

[44] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-Up SRAM state as an identifying fingerprint and source of true reandom numbers," *IEEE Trans. on Computers*, vol. 58, no. 9, pp. 1198–1210, Sept. 2009.

[45] A. Juels, R. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," in *Proc. of Computer and Communications Security Conf.*, Washington, DC, Oct. 2003.

[46] G. Karjoth and P. Moskowitz, "Disabling RFID tags with visible confirmation: Clipped tags are silenced," in *Proc. of ACM Workshop on Privacy in the Electronic Society*, Alexandria, VA, Nov. 2005.

[47] S. Inoue and H. Yasouura, "RFID privacy using user-controllable uniqueness," in *Proc. of RFID Privacy Workshop*, Boston, MA, Nov. 2003.

[48] D. Shih, R. Sun, D. Yen, and S. Huang, "Taxonomy and survey of RFID anti-collision protocols," *Computer Communications*, vol. 29, no. 11, pp. 2150–2166, July 2006.

[49] J. Myung and W. Lee, "Adaptive splitting protocols for RFID tag collision arbitration," in *Proc. of ACM MobiHoc*, Florence, Italy, May 2006.

[50] Y.-C. Ko, S. Roy, J. R. Smith, H.-W. Lee, and C.-H. Cho, "An enhanced dynamic RFID multiple access protocol for fast inventory," in *Proc. of IEEE Globecom*, Washington, DC, Nov. 2007.

[51] J. S. Choi, H. Lee, D. W. Engels, and R. Elmasri, "Robust and dynamic bin slotted anti-collision algorithms in RFID systems," in *Proc. of IEEE Int'l Conf. on RFID*, Las Vegas, NV, Apr. 2008.

[52] H. Koh, S. Yun, and H. Kim, "Sidewalk: A RFID tag anti-collision algorithm exploiting sequential arrangements of tags," in *Proc. of IEEE ICC*, Beijing, China, May 2008.

[53] J.-B. Eom, T.-J. Lee, R. Rietman, and A. Yener, "Efficient framed-slotted Aloha algorithm with pilot frame and binary selection for anti-collision of RFID tags," *IEEE Communications Letters*, vol. 12, no. 11, pp. 861–863, Nov. 2008.

[54] C.-H. Quan, J.-C. Choi, G.-Y. Choi, and C.-W. Lee, "The Slotted-LBT: A RFID reader medium access scheme in dense reader environments," in *Proc. of IEEE Int'l Conf. on RFID*, Las Vegas, NV, Apr. 2008.

[55] C. Floerkemeier, "Bayesian transmission strategy for framed ALOHA based RFID protocols," in *Proc. of IEEE RFID Conf.*, Grapevine, TX, Mar. 2007.

[56] G. Mazurek, "Active RFID system with spread-spectrum transmission," *IEEE Trans. on Automation Science and Engineering*, vol. 6, no. 1, pp. 25–32, Jan. 2009.

[57] Y. Lai and C. Lin, "Two blocking algorithms on adaptive binary splitting: Single and pair resolution for RFID tag identification," *IEEE/ACM Trans. on Networking*, vol. 17, no. 3, pp. 962–975, June 2009.

[58] H. Wu and Y. Zeng, "Efficient framed slotted aloha protocol for RFID tag anti-collision," *IEEE Trans. on Automation Science and Engineering*, vol. 8, no. 3, pp. 581–588, July 2011.

[59] Y. Lai and L. Y. Hsiao, "General binary tree protocol for coping with the capture effect in RFID tag identification," *IEEE Communications Letters*, vol. 14, no. 3, pp. 208–210, Mar. 2010.

[60] G. Mazurek, "Design of RFID system with DS-CDMA transmission," in *Proc. of IEEE CASE*, Washington DC, Aug. 2008.

[61] C. Mutti and C. Floerkemeier, "CDMA-based RFID systems in dense scenarios: Concepts and challenges," in *Proc. of IEEE RFID*, Las Vegas, NV, Apr. 2008.

[62] T. Demeechai and S. Siwamogsatham, "Using CDMA to enhance the MAC performance of ISO/IEC 18000-6 type C," *IEEE Communications Letters*, vol. 15, no. 10, pp. 1129–1131, Oct. 2011.

[63] J. Y. Maina, M. H. Mickle, M. R. Lovell, and L. A. Schaefer, "Application of CDMA for anti-collision and increased read efficiency of multiple RFID tags," *Journal of Manufacturing Systems*, vol. 26, no. 1, pp. 37–43, June 2008.

[64] H. Liu, M. Bolic, A. Nayak, and I. Stojmenovic, "Taxonomy and challenges of the integration of RFID and wireless sensor networks," *IEEE Networks*, vol. 22, no. 6, pp. 26–35, Dec. 2008.

[65] L. Wuu, Y. Chen, C. Hung, and W. Kuo, "Zero-collision RFID tags identification based on CDMA," in *Proc. of IAS*, Xian, China, Aug. 2009.

[66] A. Loeffler, F. Schuh, and H. Gerhaeuser, "Realization of a CDMA-based system using a semi-active UHF transponder," in *Proc. of ICWMC*, Valencia, Spain, Sept. 2010.

[67] P. Wang, A. Hu, and W. Pei, "The design of anti-collision mechanism of UHF RFID system based on CDMA," in *Proc. of IEEE APCCAS*, Singapore, Dec. 2006.

[68] T. S. L. Porta, G. Maselli, and C. Petrioli, "Anticollision protocols for single-reader RFID systems: Temporal analysis and optimization," *IEEE Trans. on Mobile Computing*, vol. 10, no. 2, pp. 267–279, Feb. 2011.

[69] H. Vogt, "Efficient object identification with passive RFID tags," in *Proc. of Int'l Conf. on Pervasive Computing*, Zurich, Switzerland, Aug. 2002.

[70] J.-B. Eom and T.-J. Lee, "Accurate tag estimation for dynamic framed-slotted aloha in rfid systems," *IEEE Communications Letters*, vol. 14, no. 1, pp. 60–62, Jan. 2010.

[71] C.-F. Lin and F. Y.-S. Lin, "Efcient estimation and collision-group-based anticollision algorithms for dynamic frame-slotted aloha in rfid networks," *IEEE Trans. on Automation Science and Engineering*, vol. 7, no. 4, pp. 840–848, Oct. 2010.

[72] M. Kodialam and T. Nandagopal, "Fast and reliable estimation schemes in RFID systems," in *Proc. of ACM Mobicom Conf.*, Los Angeles, CA, Sept. 2006.

[73] J. Park, M. Y. Chung, and T. J. Lee, "Identification of RFID tags in framed-slotted ALOHA with robust estimation and binary selection," *IEEE Commun. Letters*, vol. 11, pp. 452–454, May 2007.

[74] H. Wu and Y. Zeng, "Bayesian tag estimate and optimal frame length for anti-collision ALOHA RFID system," *IEEE Trans. on Automation Science and Engineering*, vol. 7, no. 4, 0.

[75] I. Onat and A. Miri, "A tag count estimation algorithm for dynamic framed ALOHA based RFID MAC protocols," in *Proc. of IEEE ICC*, Kyoto, Japan, June 2011.

[76] EPCglobal, "EPC Radio-Frequency Identity Protocols: EPC Class-1 HF RFID Air Interface Protocol for Communications at 13.56 MHz," 2011. [Online]. Available: http://www.gs1.org/sites/default/files/docs/epcglobal/epcglobal_hf_2_0_3-standard-20110905r3.pdf

[77] L. Hanzo and M. M *OFDM and MC-CDMA for Broadcasting Multi-user Communications, WLANs and Broadcasting*. John Wiley, 2003.

[78] R. Prasad and T. Ojanpera, "An overview of CDMA evolution toward wideband CDMA," *IEEE Communications Surveys*, vol. 1, no. 1, pp. 2–29, Mar. 1998.

[79] E. Vahedi, V. Shah-Mansouri, V. Wong, and I. F. Blake, "A probabilistic approach for detecting blocking attack in RFID systems," in *Proc. of IEEE ICC*, Cape Town, South Africa, May 2010.

[80] E. Vahedi, R. K. Ward, V. Shah-Mansouri, V. W. Wong, and I. F. Blake, "On securing RFIDs against blocking attacks," *IEEE MMTC Letter*, vol. 2, no. 6, pp. 16–18, Dec. 2011.

[81] E. Vahedi, R. K. Ward, and I. F. Blake, "Security analysis and complexity comparison of some recent light-weight RFID protocols," in *LNCS 6694 (Springer-Heidelberg)*, Malaga, Spain, June 2011.

[82] ——, "Toward a secure light-weight protocol for RFID systems," *IET Journal of Information Security*, submitted.

[83] E. Vahedi, V. Wong, and I. F. Blake, "A note on a probabilistic analysis of an accurate tag estimate method," *IEEE Trans. on Automation Science and Engineering*, vol. 8, no. 3, pp. 659–663, July 2011.

[84] E. Vahedi, R. K. Ward, and I. F. Blake, "Analytical modeling of RFID generation-2 protocol using absorbing markov chain theorem," in *Proc. of IEEE Globecom*, Anaheim, CA, Dec. 2012.

[85] ——, "Analytical modeling and performance analysis of RFID generation-2 protocol," *IEEE Trans. on Wireless Communications*, submitted.

[86] ——, "Performance analysis of RFID protocols: CDMA vs. the standard EPC Gen-2," *IEEE Trans. on Automation Science and Engineering*, submitted.

[87] *Draft protocol specification for a 900 MHz class 0 Radio Frequency Identification Tag*. Auto-ID Center, 2003.

[88] J. Ryu, H. Lee, Y. Seok, T. Kwon, and Y. Choi, "A hybrid query tree protocol for RFID systems," in *Proc. of IEEE ICC*, China, June 2007.

[89] S. S. Choi, Y. S. Hong, and S. K. Kim, "Dynamic framed ALOHA algorithm using a collision factor in RFID systems," in *Proc. of IEEE VTC-Fall*, Barcelona, Spain, Sept. 2009.

[90] D. Liu, Z. Wang, J. Tan, H. Min, and J. Wang, "ALOHA algorithm considering the slot duration difference in RFID system," in *Proc. of IEEE RFID Conf.*, Orlando, FL, Apr. 2009.

[91] I. Onat and A. Miri, "DiSEL: A distance based slot selection protocol for framed slotted ALOHA RFID systems," in *Proc. of IEEE WCNC*, Budapest, Hungary, Apr. 2009.

[92] S. Geng, D. M. Gao, C. Zhu, M. He, and W. C. Wu, "An improved dynamic framed slotted ALOHA algorithm for RFID anti-collision," in *Proc. of IEEE ICSP*, Leipzig, Germany, Oct. 2008.

[93] M. Kodialam, T. Nandagopal, and W. C. Lau, "Anonymous tracking using RFID tags," in *Proc. of IEEE Infocom*, Anchorage, AK, May 2007.

[94] M. Roberti, "Wal-Mart relaunches EPC RFID effort, starting with men's jeans and basics," *RFID Journal*, July 2010.

[95] W. Feller, *An Introduction to Probability Theory and Its Applications*. John Wiley, 1957.

[96] J. Riordan, *An Introduction to Combinatorial Analysis*. John Wiley, 1958.

[97] G. Avoine and P. Oechslin, "RFID traceability: A multilayer problem," in *Proc. of Financial Cryptography and Data Security*, Roseau, Dominica, Feb. 2005.

[98] A. Shamir, "SQUASH-A new MAC with provable security properties for highly constrained devices such as RFID tags," in *Proc. of FSE*, Lausanne, Switzerland, Feb. 2008.

[99] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, Nov 1981.

[100] M. Feldhofer and C. Rechberger, "A case against currently used hash functions in RFID protocols," in *Proc. of RFID Security*, Graz, Austria, Sept. 2006.

[101] D. Engels, X. Fan, G. Gong, H. Hu, and E. M. Smith, "Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices," in *Proc. of FCDS*, Tenerife, Spain, Jan. 2010.

[102] D. Engels, M. O. Saarinen, P. Schweitzer, and E. M. Smith, "The Hummingbird-2 Lightweight Authenticated Encryption Algorithm," in *Proc. of RFIDSec*, Amherst, MA, June 2011.

[103] X. Fan, G. Gong, K. Lauffenburger, and T. Hicks, "FPGA Implementations of the Hummingbird Cryptographic Algorithm," in *Proc. of HOST*, Anaheim, CA, June 2010.

[104] M. Hell, T. Johansson, A. Maximov, and W. Meier, "A stream cipher proposal: Grain-128," in *Proc. of ISIT*, Seattle, WA, July 2006.

[105] J. P. Aumasson, L. Henzen, W. Meier, and M. N. Plasencia, "QUARK: a Lightweight Hash," in *Proc. of CHES*, Santa Barbara, CA, Aug. 2010.

[106] M. O. Rabin, *Digitized Signatures and Public-Key Functions as Intractable as Factorization.* MIT-TR 212, 1979.

[107] J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel, "A new RFID privacy model," in *Proc. of ESORICS*, Leuven, Belgium, Sept. 2011.

[108] R. Deng, Y. Li, M. Yung, and Y. Zhao, "A new framework for RFID privacy," in *Proc. of ESORICS*, Athens, Greece, Sept. 2010.

[109] A. Juels and S. A. Weis, "Defining strong privacy for RFID," in *Proc. of PerCom*, New York, USA, Mar. 2007.

[110] S. Vaudenay, "On privacy models for RFID," in *Proc. of ASIACRYPT*, Kuching, MALAYSIA, Dec. 2007.

[111] S. Wang, W. Hong, L. Yin, and S. Li, "A novel fast tag estimate method for dynamic frame length aloha anti-collision algorithms in RFID system," in *Proc. of IEEE VTC*, Quebec City, Canada, Sept. 2012.

[112] S.-D. J. S.-R. Lee and C.-W. Lee, "An enhanced dynamic framed aloha algorithm for RFID tag identication," in *Proc. of MOBIQUITOUS*, San Diego, CA, July 2005.

[113] C. Quan, Y. Liu, H. Ngan, and L. M. Ni, "ASAP: Scalable identification and counting for contactless RFID systems," in *Proc. of ICDCS*, Genoa, Italy, June 2010.

[114] Y. Zheng and M. Li, "PET: Probabilistic estimating tree for large-scale RFID estimation," *IEEE Trans. on Mobile Computing*, vol. 11, no. 11, pp. 1763–1774, Nov. 2012.

[115] H. Han, B. Sheng, C. C. Tan, Q. Li, W. Mao, and S. Lu, "Counting RFID tags efficiently and anonymously," in *Proc. of IEEE INFOCOM*, San Diego, CA, Mar. 2010.

[116] C. Qian, H. Ngan, and Y. Liu, "Cardinality estimation for large-scale RFID systems," in *Proc. of PerCom*, Hong Kong, Mar. 2008.

[117] Y. Sun, P. J. Hawrylak, and M. H. Mickle, "Application of ICA in collision resolution for passive RFID communication," in *Proc. of WCECS*, San Fransisco, CA, Oct. 2009.

[118] Y. Maguire and R. Pappu, "An optimal Q-algorithm for ISO 18000-6C UHF RFID," *IEEE Trans. on Automation Science and Engineering*, vol. 6, no. 1, pp. 16–24, Nov. 2009.

[119] H. Hirayama, Y. Satake, N. Kihuma, and K. Sakakibara, "Improvement of null zone avoidance capability for HF-band RFID using diversity combining of loop antennas," in *Proc. of 3rd European Conference on Antennas and Propagation*, Berlin, Germany, Mar. 2009.

[120] J. G. Kim, W. J. Shih, and J. H. Yoo, "Performance analysis of EPC class-1 generation-2 RFID anti-collision protocol," *LNCS, Springer*, vol. 4707, pp. 1017–1026, Aug. 2007.

[121] J. G. Proakis and M. Salehi, *Communication Systems Engineering*. Prentice Hall, 2003.

[122] Passport-Canada. [Online]. Available: http://www.ppt.gc.ca/eppt/about.aspx?lang=eng