SECURITY AND COLLISION IN RFID SYSTEMS

by

Mohammed Jameel Hakeem

MASc, University of Waterloo, Waterloo, Canada, 2008

BASc, King Abdul-Aziz University, Jeddah, Saudi Arabia, 2004

A dissertation

Presented to Ryerson University

in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

in the Program of

Electrical and Computer Engineering

Toronto, Ontario, Canada, 2015

©Mohammed Jameel Hakeem 2015

SECURITY AND COLLISION IN RFID SYSTEMS

by

Mohammed Jameel Hakeem MASc, University of Waterloo, Waterloo, Canada, 2008 BAsC,
King Abdul-Aziz University, Jeddah, Saudi Arabia, 2004

A dissertation

Presented to Ryerson University

in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

in the Program of

Electrical and Computer Engineering

Toronto, Ontario, Canada, 2015

©Mohammed Jameel Hakeem 2015

Author's Declaration

AUTHOR'S DECLARATION FOR ELECTRONIC SUBMISSION OF A DISSERTATION

I hereby declare that I am the sole author of this dissertation. This is a true copy of the dissertation, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this dissertation to other institutions or individuals for the purpose of scholarly research

I further authorize Ryerson University to reproduce this dissertation by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my dissertation may be made electronically available to the public.

DISSERTATION

I hereby declare that I am the sole author of this dissertation. This is a true copy of the dissertation, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this dissertation to other institutions or individuals for the purpose of scholarly research

I further authorize Ryerson University to reproduce this dissertation by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my dissertation may be made electronically available to the public.

Abstract

Radio Frequency Identification (RFID) is a promising technology to provide automated contactless identification of objects, people and animals. The identification process is performed as the reader receives simultaneous responses from various tags over a shared wireless channel and without no requirement of line-of-sight in the interrogation zone. The communication between the reader and tags is separated into two processes: identification and acknowledgment processes. Both processes suffer from serious drawbacks that limit the proliferation of RFID. Such drawbacks are security and privacy and collision problems.

This thesis has two main parts. The first part examines the security and privacy of the existing RFID authentication protocols. We introduced a novel cryptographic scheme, Hacker Proof Authentication Protocol (HPAP) that allows mutual authentication and achieves full security by deploying tag static identifier, updated timestamp, a one-way hash function and encryption keys with randomized update using Linear Feedback Shift Register (LFSR). Cryptanalysis and simulation show that the protocol is secure against various attacks. In comparison with the various existing RFID authentication protocols, our protocol has less computation load, requires less storage, and costs less.

The second part focuses on solving RFID collision arbitration imposed by the shared wireless link between a reader and the many tags distributed in the interrogation zone. In most proposed anti-collision algorithms, tags reply randomly to the time slots chosen by the reader. Since more than two tags may choose the same time slot in a frame, this Random Access (RA) causes garbled data at the reader side resulting the identification process fails. Towards this challenge, two ALOHA based anti-collision algorithms that adopt a new way for tags to choose their replied time slots to enhance system efficiency are presented. In MBA and LT MBA, tags use *modulo* function to choose their owned time slot. The difference between the two algorithms relies on the method by which the reader estimates the next frame size. The performance evaluation of the two algorithms shows better performance than previously proposed algorithms in terms of fewer communication rounds and fewer collided/empty slots considering the limitation of the EPCglobal Class-1 Gen-2 standard.

Computer Engineering, Ryerson University.

Abstract Radio Frequency Identification (RFID) is a promising technology to provide automated contactless identification of objects, people and animals. The identification process is performed as the reader receives simultaneous responses from various tags over a shared wireless channel and without no requirement of line-of-sight in the interrogation zone. The communication between

the reader and tags is separated into two processes: identification and acknowledgment processes.

Both processes suffer from serious drawbacks that limit the proliferation of RFID. Such drawbacks

are security and privacy and collision problems.

This thesis has two main parts. The first part examines the security and privacy of the existing RFID authentication protocols. We introduced a novel cryptographic scheme, Hacker Proof Authentication Protocol (HPAP) that allows mutual authentication and achieves full security by deploying tag static identifier, updated timestamp, a one-way hash function and encryption keys with randomized update using Linear Feedback Shift Register (LFSR). Cryptanalysis and simulation show that the protocol is secure against various attacks. In comparison with the various

existing RFID authentication protocols, our protocol has less computation load, requires less storage, and costs less.

The second part focuses on solving RFID collision arbitration imposed by the shared wireless link

between a reader and the many tags distributed in the interrogation zone. In most proposed anti-collision algorithms, tags reply randomly to the time slots chosen by the reader. Since more than two tags may choose the same time slot in a frame, this Random Access (RA) causes garbled data

at the reader side resulting the identification process fails. Towards this challenge, two ALOHA based anti-collision algorithms that adopt a new way for tags to choose their replied time slots to enhance system efficiency are presented. In MBA and LT MBA, tags use modulo function to choose their owned time slot. The difference between the two algorithms relies on the method by which the reader estimates the next frame size. The performance evaluation of the two

algorithms

shows better performance than previously proposed algorithms in terms of fewer communication rounds and fewer collided/empty slots considering the limitation of the EPCglobal Class-1 Gen-2 standard.

iii

Acknowledgment

First of all, I am grateful to God (Allah), The Most Beneficent, The Most Merciful. Him and only gave me and keeps giving me the strength to bring out the best of me to success in life.

It is difficult to overstate my gratitude to my Ph.D. supervisors, Dr. Kaamran Raahemifar and Dr. Gul Khan. Their enthusiasm, inspiration, and great efforts to explain things clearly and simply, have helped me to better understand the field of security and optimization. Throughout my thesis-writing period, Dr. Kamran provided encouragement, sound advice, good teaching, good company, and many good ideas. I truly would have been lost without him. It was an honor and a privilege to work under the joint supervision of Dr. Kaamran Raahemifar and Dr. Gul Khan. In addition, I would like to extend my gratitude to my PhD defense committee; Chair - Dr. Paul Moore, External – Dr. Mustapha Yagoub, Dr. Alagan Anpalagan, Dr. Alireza Sadeghian, Dr. Nagi Mekhiel for their valuable comments in the internal and external defense.

My deepest gratitude extend to the Government of the Kingdom of Saudi Arabia, for the great chance to pursue my graduate studies through the custodian of the two holy mosques scholarship program and King Abdul-Aziz University. Many Thanks every and single supervisor I dealt with at the Saudi cultural Bureau in Ottawa. I specifically want to thank, Dr. Faisal Aba-Al-Khail, Dr. Ali Al-Bishri, Dr. Nasser Al-Shalaan, Dr. Amal Alamoudi, Dr. Samiah Al-Jabri and my supervisor Suha Mansour. Finally, I want to thank Dr. Majid Alotaibi, Dr. Danilo Yu, Eng. Haitham Turkistani for their help towards my research.

Certain people have giving me ultimate support and encouragement, having them in my live is a bless. Thank you to my beloved wife Maram Bajri; she was the best support to me every second. My great thanks to my all friends who never hesitated to give me valuable advises in life and school. Specifically, Dr. Omar Attas, Dr. Nezar Bahabri, Dr. Hassan Huwait, Dr. Abdullah Aldammak, Dr. Rami Kinsara and Enrique.

Lastly, I am extremely grateful to my family, Mom (Najiya), Essra, Bassem, Yasser, Hamza, battal and little cute Miral for their constant support and encouragement.

Merciful. Him and only

gave me and keeps giving me the strength to bring out the best of me to success in life.

It is difficult to overstate my gratitude to my Ph.D. supervisors, Dr. Kaamran Raahemifar and Dr. Gul Khan. Their enthusiasm, inspiration, and great efforts to explain things clearly and simply, have helped me to better understand the field of security and optimization. Throughout my thesis-

writing period, Dr. Kamran provided encouragement, sound advice, good teaching, good company,

and many good ideas. I truly would have been lost without him. It was an honor and a privilege to

work under the joint supervision of Dr. Kaamran Raahemifar and Dr. Gul Khan. In addition, I would like to extend my gratitude to my PhD defense committee; Chair - Dr. Paul Moore, External

– Dr. Mustapha Yagoub, Dr. Alagan Anpalagan, Dr. Alireza Sadeghian, Dr. Nagi Mekhiel for their

valuable comments in the internal and external defense.

My deepest gratitude extend to the Government of the Kingdom of Saudi Arabia, for the great chance to pursue my graduate studies through the custodian of the two holy mosques scholarship program and King Abdul-Aziz University. Many Thanks every and single supervisor I dealt with at the Saudi cultural Bureau in Ottawa. I specifically want to thank, Dr. Faisal Aba-Al-Khail, Dr. Ali Al-Bishri, Dr. Nasser Al-Shalaan, Dr. Amal Alamoudi, Dr. Samiah Al-Jabri and my supervisor

Suha Mansour. Finally, I want to thank Dr. Majid Alotaibi, Dr. Danilo Yu, Eng. Haitham Turkistani for their help towards my research.

Certain people have giving me ultimate support and encouragement, having them in my live is a bless. Thank you to my beloved wife Maram Bajri; she was the best support to me every second. My great thanks to my all friends who never hesitated to give me valuable advises in life and school. Specifically, Dr. Omar Attas, Dr. Nezar Bahabri, Dr. Hassan Huwait, Dr. Abdullah Aldammak, Dr. Rami Kinsara and Enrique.

Lastly, I am extremely grateful to my family, Mom (Najiya), Essra, Bassem, Yasser, Hamza, battal

and little cute Miral for their constant support and encouragement.

iv

Dedication

To

My Dad "Jameel" who never get to see this moment

I miss you baba - RIP

Dedication

To

My Dad “Jameel” who never get to see this moment

I miss you baba - RIP

v

Table of Contents

Author's Declaration.....	ii
Abstract.....	iii
Acknowledgment.....	iv
Dedication.....	v
Table of Contents.....	vi
List of Tables.....	x
List of Figures.....	xi
List of Symbols and Abbreviation.....	xiv
1. Chapter 1.....	1
Motivation and Contributions.....	1
1.1 Motivation.....	1
1.2 Objectives.....	3
1.3 Thesis Organization.....	4
2. Chapter 2.....	6
Introduction to Radio Frequency Identification.....	6
2.1 History.....	6
2.2 RFID System Structure.....	7
2.2.1 RFID Tags.....	8
2.2.2 RFID Readers.....	9
2.2.3 Back-end Server.....	9
2.3 RFID Standards.....	10
2.4 RFID Applications.....	11
2.4.1 Supply chain management applications.....	11
2.4.2 Access Control applications.....	11

.....	ii
Abstract	iii
Acknowledgment	iv
Dedication	v
Table of Contents	vi
List of Tables	x
List of Figures	xi
List of Symbols and Abbreviation	xiv
1. Chapter 1	1
Motivation and Contributions	1
1.1 Motivation	1
1.2 Objectives	3
1.3 Thesis Organization.....	4
2. Chapter 2	6
Introduction to Radio Frequency Identification	6
2.1 History.....	6
2.2 RFID System Structure	7
2.2.1 RFID Tags	8
2.2.2 RFID Readers.....	9
2.2.3 Back-end Server	9
2.3 RFID Standards	10
2.4 RFID Applications	11

2.4.1 Supply chain management applications	11
2.4.2 Access Control applications	11

2.4.3 Cashless Payment Applications	12
2.4.4 Animal and human tracking applications	13
2.4.5 Healthcare Industry Applications	14
3. Chapter 3.....	16
Privacy and Authentication in Radio Frequency Identification.....	16
3.1 Privacy	16
3.2 Privacy requirements	17
3.3 Authentication.....	17
3.4 Attacks on RFID system	18
3.5 Providing Security Requirements	19
3.6 RFID Privacy and Authentication Protocols.....	20
3.6.1 Tag Killing approach	20
3.6.2 Cryptography approach.....	21
3.7 An Overview on RFID Authentication Protocols.....	22
3.7.1 Tag Computational Effort.....	22
3.7.2 Tag Storage Capabilities	22
3.7.3 Number of Rounds	22
3.7.4 Scalability	22
3.8 Related Work	23
3.8.1 Hash Function Based Authentication Protocols	23
3.8.2 Lightweight Based Authentication Protocols	27
3.8.3 Ultralightweight Authentication Protocol.....	36
3.9 Conclusion	41
4. Chapter 4.....	43
Collision in Radio Frequency Identification Systems	43

2.4.4 Animal and human tracking applications	13
2.4.5 Healthcare Industry Applications	14
3. Chapter 3	16
Privacy and Authentication in Radio Frequency Identification	16
3.1 Privacy	16
3.2 Privacy requirements	17
3.3 Authentication	17
3.4 Attacks on RFID system	18
3.5 Providing Security Requirements	19
3.6 RFID Privacy and Authentication Protocols.....	20
3.6.1 Tag Killing approach	20
3.6.2 Cryptography approach	21
3.7 An Overview on RFID Authentication Protocols	22
3.7.1 Tag Computational Effort	22
3.7.2 Tag Storage Capabilities	22
3.7.3 Number of Rounds	22
3.7.4 Scalability	22
3.8 Related Work	23
3.8.1 Hash Function Based Authentication Protocols	23
3.8.2 Lightweight Based Authentication Protocols	27
3.8.3 Ultralightweight Authentication Protocol	36
3.9 Conclusion	41
4. Chapter 4	43
Collision in Radio Frequency Identification Systems	43

4.1 Introduction.....	43
4.2 Estimation Techniques and Anti-Collision Protocols.....	44
4.2.1 Estimation Techniques.....	44
4.2.2 Tag Anti-Collision Algorithms.....	48
4.3 Conclusion	61
5. Chapter 5.....	62
Key Management Protocol for Radio Frequency Identification Systems	62
5.1 Authentication Protocol Parameters	62
5.2 Operating Environment.....	63
5.3 HPAP Component.....	64
5.4 System Model	65
5.4.1 HPAP Set up and Assumptions.....	65
5.4.2 Notation.....	66
5.4.3 Protocol description	66
5.5 Protocol Analysis and Simulation.....	68
5.5.1 Performance Analysis	68
5.5.2 Computer Simulation.....	70
5.5.3 Hardware Implementation	71
5.5.4 Security Analysis	78
5.6 Conclusion	83
6. Chapter 6.....	84
Modulo based Aloha Anti-Collision Algorithms for Radio Frequency Identification Systems...	84
6.1 EPC GLOBAL CLASS 1 GENERATION 2 STANDARD.....	84
6.2 Fundamental Theory	86
6.3 Mathematical Model	86

4.2 Estimation Techniques and Anti-Collision Protocols	44
4.2.1 Estimation Techniques	44
4.2.2 Tag Anti-Collision Algorithms	48
4.3 Conclusion	61
5. Chapter 5	62
Key Management Protocol for Radio Frequency Identification Systems	62
5.1 Authentication Protocol Parameters	62
5.2 Operating Environment	63
5.3 HPAP Component	64
5.4 System Model	65
5.4.1 HPAP Set up and Assumptions.....	65
5.4.2 Notation.....	66
5.4.3 Protocol description	66
5.5 Protocol Analysis and Simulation	68
5.5.1 Performance Analysis	68
5.5.2 Computer Simulation	70
5.5.3 Hardware Implementation	71
5.5.4 Security Analysis	78
5.6 Conclusion	83
6. Chapter 6	84
Modulo based Aloha Anti-Collision Algorithms for Radio Frequency Identification Systems ...	84
6.1 EPC GLOBAL CLASS 1 GENERATION 2 STANDARD	84
6.2 Fundamental Theory	86
6.3 Mathematical Model	86

6.4 Estimation Techniques.....	87
6.5 Modulo Tag Anti-Collision Algorithm.....	88
6.6 Look-up Modulo Tag Anti-Collision Algorithm	90
6.7 Algorithms Analysis	93
6.7.1 System Efficiency	93
6.7.2 System Model	94
6.8 Simulation Results	95
6.9 Conclusion	108
7. Chapter 7.....	110
Conclusion and Future Work	110
7.1 Thesis Contributions	110
7.1.1 Summary	110
7.1.2 Thesis organization details.....	111
7.2 Future Work	113
8. Appendix A.....	115
9. Appendix B	118
10. References.....	128

6.5 Modulo Tag Anti-Collision Algorithm	88
6.6 Look-up Modulo Tag Anti-Collision Algorithm	90
6.7 Algorithms Analysis	93
6.7.1 System Efficiency	93
6.7.2 System Model	94
6.8 Simulation Results	95
6.9 Conclusion	108
7. Chapter 7	110
Conclusion and Future Work	
110	
7.1 Thesis Contributions	110
7.1.1 Summary	110
7.1.2 Thesis organization details	111
7.2 Future Work	113
8. Appendix A	115
9. Appendix B	118
10. References	128

List of Tables

Table 4.1 Tag Anti-Collision Algorithms Comparison	59
Table 5.1 HPAP Notation	66
Table 5.2 Comparing the memory storage offered by HPAP and other authentication protocols	68
Table 5.3 Comparing the communication cost of HPAP with that of other authentication protocols.....	69
Table 5.4 Comparing the computational load of HPAP protocol with that of other authentication protocols.....	70
Table 5.5 Comparing the security offered by HPAP and other authentication protocols.....	83
Table 6.1 A Sample of the Pre-Saved Reader's Table.....	92
Table 6.2 Proposed Anti-collision algorithms comparison; for 8 tags and initial NF=4.....	96
Table 6.3 Comparing different anti-collision algorithms; for 1000 tags and initial NF=32.....	103

.....	59
Table 5.1 HPAP Notation	66
Table 5.2 Comparing the memory storage offered by HPAP and other authentication protocols	68
Table 5.3 Comparing the communication cost of HPAP with that of other authentication protocols	69
Table 5.4 Comparing the computational load of HPAP protocol with that of other authentication protocols	70
Table 5.5 Comparing the security offered by HPAP and other authentication protocols	83
Table 6.1 A Sample of the Pre-Saved Reader's Table	92
Table 6.2 Proposed Anti-collision algorithms comparison; for 8 tags and initial NF=4	96
Table 6.3 Comparing different anti-collision algorithms; for 1000 tags and initial NF=32	103
x	