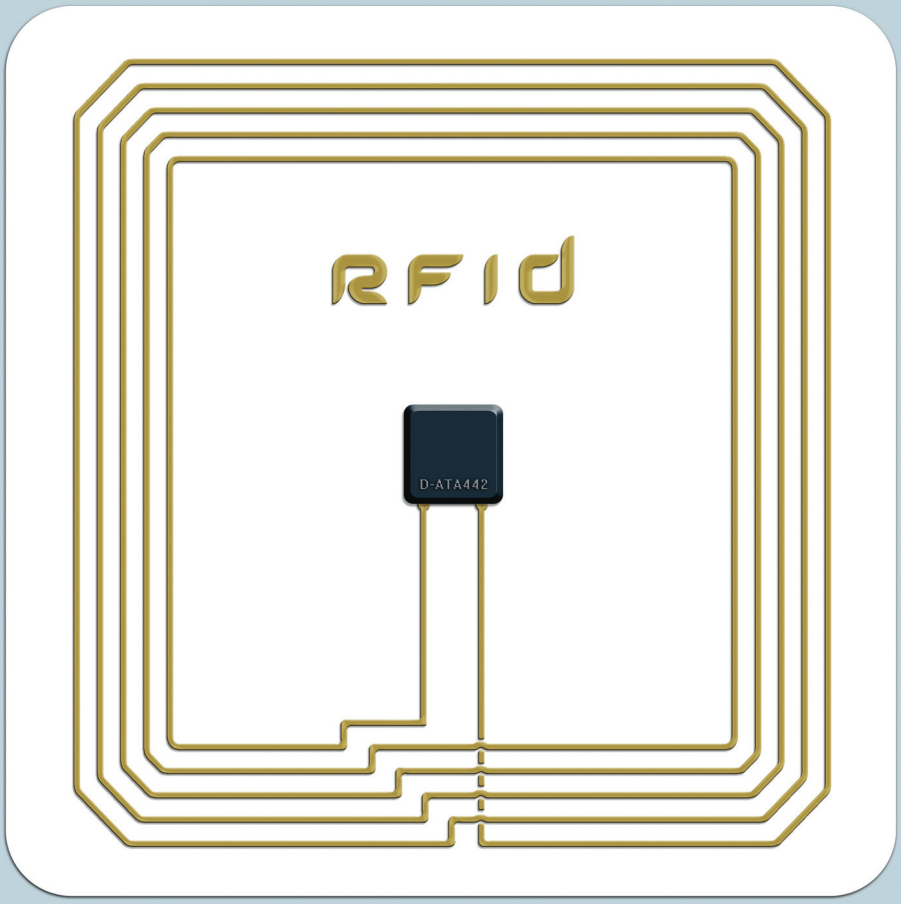
Wireless Networks and Mobile Communications Series

Security in RFID and Sensor Networks

Edited by Yan Zhang ♦ Paris Kitsos



CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Security in RFID and Sensor Networks

WIRELESS NETWORKS AND MOBILE COMMUNICATIONS

Dr. Yan Zhang, Series Editor
Simula Research Laboratory, Norway
E-mail: yanzhang@ieee.org

Broadband Mobile Multimedia: Techniques and Applications
Yan Zhang, Shiwen Mao, Laurence T. Yang, and Thomas M Chen
ISBN: 978-1-4200-5184-1

Cooperative Wireless Communications
Yan Zhang, Hsiao-Hwa Chen, and Mohsen Guizani
ISBN: 978-1-4200-6469-8

Distributed Antenna Systems: Open Architecture for Future Wireless Communications
Honglin Hu, Yan Zhang, and Jijun Luo
ISBN: 978-1-4200-4288-7

The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems
Lu Yan, Yan Zhang, Laurence T. Yang, and Huansheng Ning
ISBN: 978-1-4200-5281-7

Millimeter Wave Technology in Wireless PAN, LAN and MAN
Shao-Qiu Xiao, Ming-Tuo Zhou and Yan Zhang
ISBN: 978-0-8493-8227-7

Mobile WIMAX: Toward Broadband Wireless Metropolitan Area Networks
Yan Zhang and Hsiao-Hwa Chen
ISBN: 978-0-8493-2624-0

Resource, Mobility and Security Management in Wireless Networks and Mobile Communications
Yan Zhang, Honglin Hu, and Masayuki Fujise
ISBN: 978-0-8493-8036-5

Security in RFID and Sensor Networks
Yan Zhang and Paris Kitsos
ISBN: 978-1-4200-6839-9

Security in Wireless Mesh Networks
Yan Zhang, Jun Zheng and Honglin Hu
ISBN: 978-0-8493-8250-5

Unlicensed Mobile Access Technology: Protocols, Architectures, Security, Standards and Applications
Yan Zhang, Laurence T. Yang, and Jianhua Ma
ISBN: 978-1-4200-5537-5

Wireless Mesh Networking: Architectures, Protocols and Standards
Yan Zhang, Jijun Luo, and Honglin Hu
ISBN: 978-0-8493-7399-2

Wireless Quality-of-Service: Techniques, Standards and Applications
Maode Ma, Mieso K. Denko, and Yan Zhang
ISBN: 978-1-4200-5130-8

AUERBACH PUBLICATIONS
www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

Security in RFID and Sensor Networks

Edited by
Yan Zhang
Paris Kitsos

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20150109

International Standard Book Number-13: 978-1-4200-6840-5 (eBook - PDF)

Contents

Editors

Yan Zhang received his BS in communication engineering from Nanjing University of Post and Telecommunications, China; his MS in electrical engineering from Beijing University of Aeronautics and Astronautics, China; and his PhD in the School of Electrical & Electronics Engineering, Nanyang Technological University, Singapore. He is an associate editor on the editorial board of *Wiley Wireless Communications and Mobile Computing* (*WCMC*); *Security and Communication Networks* (Wiley); *International Journal of Network Security; International Journal of Ubiquitous Computing*; *Transactions on Internet and Information Systems* (*TIIS*); *International Journal of Autonomous and Adaptive Communications Systems* (*IJAACS*); *International Journal of Ultra Wideband Communications and Systems* (*IJUWBCS*); and *International Journal of Smart Home* (*IJSH*). He is currently serving as the book series editor for Wireless Networks and Mobile Communications book series (Auerbach Publications, CRC Press, Taylor & Francis Group). He serves as guest coeditor for the following: *IEEE Intelligent Systems*, special issue on "Context-Aware Middleware and Intelligent Agents for Smart Environments"; *Wiley Security and Communication Networks* special issue on "Secure Multimedia Communication"; *Springer Wireless Personal Communications* special issue on selected papers from ISWCS 2007; *Elsevier Computer Communications* special issue on "Adaptive Multicarrier Communications and Networks"; *International Journal of Autonomous and Adaptive Communications Systems* (*IJAACS*) special issue on "Cognitive Radio Systems"; *The Journal of Universal Computer Science* (*JUCS*) special issue on "Multimedia Security in Communication"; *Springer Journal of Cluster Computing* special issue on "Algorithm and Distributed Computing in Wireless Sensor Networks"; *EURASIP Journal on Wireless Communications and Networking* (*JWCN*) special issue on "OFDMA Architectures, Protocols, and Applications"; and *Springer Journal of Wireless Personal Communications* special issue on "Security and Multimodality in Pervasive Environments."

He is serving as coeditor for several books: *Resource, Mobility and Security Management in Wireless Networks and Mobile Communications*; *Wireless Mesh Networking: Architectures, Protocols and Standards; Millimeter-Wave Technology in Wireless PAN, LAN and MAN; Distributed Antenna Systems: Open Architecture for Future Wireless Communications; Security in Wireless Mesh Networks; Mobile WiMAX: Toward Broadband Wireless Metropolitan Area Networks; Wireless Quality-of-Service: Techniques, Standards and Applications; Broadband Mobile Multimedia: Techniques and Applications; Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems; Unlicensed Mobile Access Technology: Protocols, Architectures, Security, Standards and Applications; Cooperative Wireless Communications; WiMAX Network Planning and Optimization; RFID Security: Techniques, Protocols and System-On-Chip Design; Autonomic Computing and Networking; Security in RFID and Sensor Networks; Handbook of Research on Wireless Security; Handbook of Research on Secure Multimedia Distribution; RFID and Sensor Networks; Cognitive Radio Networks; Wireless Technologies for Intelligent Transportation Systems; Vehicular Networks: Techniques, Standards and Applications; Orthogonal Frequency Division Multiple Access (OFDMA); Game Theory for Wireless Communications and Networking; and Delay Tolerant Networks: Protocols and Applications.*

Dr. Zhang serves as symposium cochair for the following: ChinaCom 2009; program cochair for BROADNETS 2009; program cochair for IWCMC 2009; workshop cochair for ADHOCNETS 2009; general cochair for COGCOM 2009; program cochair for UC-Sec 2009; journal liasion chair for IEEE BWA 2009; track cochair for ITNG 2009; publicity cochair for SMPE 2009; publicity cochair for COMSWARE 2009; publicity cochair for ISA 2009; general cochair for WAMSNet 2008; publicity cochair for TrustCom 2008; general cochair for COGCOM 2008; workshop cochair for IEEE APSCC 2008; general cochair for WITS-08; program cochair for PCAC 2008; general cochair for CONET 2008; workshop chair for SecTech 2008; workshop chair for

SEA 2008; workshop co-organizer for MUSIC'08; workshop co-organizer for 4G-WiMAX 2008; publicity cochair for SMPE-08; international journals coordinating cochair for FGCN-08; publicity cochair for ICCCAS 2008; workshop chair for ISA 2008; symposium cochair for ChinaCom 2008; industrial cochair for MobiHoc 2008; program cochair for UIC-08; general cochair for CoNET 2007; general cochair for WAMSNet 2007; workshop cochair FGCN 2007; program vice-cochair for IEEE ISM 2007; publicity cochair for UIC-07; publication chair for IEEE ISWCS 2007; program cochair for IEEE PCAC'07; special track cochair for "Mobility and Resource Management in Wireless/Mobile Networks" in ITNG 2007; special session co-organizer for "Wireless Mesh Networks" in PDCS 2006; and a member of technical program committee for numerous international conferences, including ICC, GLOBECOM, WCNC, PIMRC, VTC, CCNC, AINA, and ISWCS. He received the Best Paper Award in the IEEE 21st International Conference on Advanced Information Networking and Applications (AINA-07).

Since August 2006, he has been working with Simula Research Laboratory, Norway (http://www.simula.no/). His research interests include resource, mobility, spectrum, data, energy, and security management in wireless networks and mobile computing. He is a member of IEEE and IEEE ComSoc.

Paris Kitsos received his BS in physics in 1999 and his PhD in 2004 from the Department of Electrical and Computer Engineering, both at the University of Patras. Since June 2005 he has been a research fellow with the Digital Systems & Media Computing Laboratory, School of Science & Technology, Hellenic Open University (HOU), Greece (http://dsmc.eap.gr/en/main.php). He is an associate editor of *Computer and Electrical Engineering* (an international journal [Elsevier]) and a member on the editorial board of *International Journal of Reconfigurable Computing* (Hindawi). He is also the coeditor of *RFID Security. Techniques, Protocols and System-On-Chip Design* published by Springer in 2008. He has participated as a program and technical committee member in more than 40 conferences and workshops in the area of his research. He has also participated as a guest coeditor in the following special issues: *Computer and Electrical Engineering* (an international journal [Elsevier Ltd]) "Security of Computers and Networks"; *Wireless Personal Communications* (an international journal [Springer]) "Information Security and Data Protection in Future Generation Communication and Networking"; and *Security and Communication Network* (SCN) (Wiley journal) "Secure Multimedia Communication."

Dr. Kitsos' research interests include VLSI design and efficient hardware implementations of cryptographic algorithms and security protocols for wireless communication systems, and hardware implementations of RFID cryptography algorithms. He is an adjunct lecturer in the Department of Computer Science and Technology, University of Peloponnese. He has published more than 60 publications in international journals, books, and technical reports, and also reviews manuscripts for books, international journals, and conferences/workshops in the areas of his research. He is also a member of the Institute of Electrical and Electronics Engineers (IEEE).

Contributors

Hossam Afifi
Mobility and Security Group
Department of Wireless Networks and Multimedia Services
Institut National des Télécommunications
Evry, France

Slobodan Bojanić
Department of Electronic Engineering
Universidad Politecnica de Madrid
Madrid, Spain

Leonid Bolotnyy
Department of Computer Science
School of Engineering and Applied Science
University of Virginia
Charlottesville, Virginia

Trevor Burbridge
British Telecommunications plc
Adastral Park, Martlesham Heath
Ipswich, United Kingdom

Aldar C.-F. Chan
Department of Computer Science
National University of Singapore
Singapore

Ioannis Chatzigiannakis
Department of Computer Engineering and Informatics
University of Patras
Patras, Greece

and

Computer Technology Institute
Patras, Greece

Hao Chen
Department of Electrical and Computer Engineering
Thomas J. Watson School of Engineering
State University of New York
Binghamton, New York

Yu Chen
Department of Electrical and Computer Engineering
Thomas J. Watson School of Engineering
State University of New York
Binghamton, New York

Xiaowen Chu
Department of Computer Science
Hong Kong Baptist University
Kowloon, Hong Kong

Tassos Dimitriou
Athens Information Technology
Athens, Greece

Alberto Peinado Domínguez
Escuela Técnica Superior de Ingenieros de Telecomunicación
University of Málaga
Málaga, Spain

Saar Drimer
Computer Laboratory
University of Cambridge
Cambridge, United Kingdom

Juan M. Estevez-Tapiador
Computer Science Department
Carlos III University of Madrid
Madrid, Spain

Jorge Munilla Fajardo
Escuela Técnica Superior de Ingenieros de Telecomunicación
University of Málaga
Málaga, Spain

Elgar Fleisch
Department of Management, Technology, and Economics
Eidgenössische Technische Hochscule
Zurich, Switzerland

and

Institute of Technology Management
University of St. Gallen
Saint Gallen, Switzerland

Sepideh Fouladgar
Mobility and Security Group
Department of Wireless Networks and Multimedia Services
Institut National des Télécommunications
Evry, France

Felix C. Freiling
Department of Informatics
University of Mannheim
Mannheim, Germany

Filippo Gandino
Dipartimento di Automatica e Informatica
Politecnico di Torino
Torino, Italy

Damianos Gavalas
Department of Cultural Technology and Communication
University of Aegean
Lesvos, Greece

Thanassis Giannetsos
Athens Information Technology
Athens, Greece

Gerhard P. Hancke
Smart Card Centre
Information Security Group
Royal Holloway University of London
London, United Kingdom

Julio Cesar Hernandez-Castro
Computer Science Department
Carlos III University of Madrid
Madrid, Spain

Jaap-Henk Hoepman
TNO Information and Communication Technology
Groningen, the Netherlands

and

Digital Security Group
Faculty of Science
Radboud University
Nijmegen, the Netherlands

Dijiang Huang
Computer Science and Engineering Department
Arizona State University
Tempe, Arizona

Alexander Ilic
Department of Management, Technology, and Economics
Eidgenössische Technische Hochschule
Zurich, Switzerland

José L. Imaña
Department of Computer Architecture and Systems Engineering
Faculty of Physics
Complutense University of Madrid
Madrid, Spain

Yixin Jiang
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, Canada

Elisavet Konstantinou
Department of Information and Communication Systems Engineering
University of the Aegean
Karlovassi, Greece

Charalampos Konstantopoulos
Department of Informatics
University of Piraeus
Piraeus, Greece

Ioannis Krontiris
Athens Information Technology
Athens, Greece

Wei-Shinn Ku
Department of Computer Science and Software Engineering
Auburn University
Auburn, Alabama

Shiguo Lian
France Telecom R&D Beijing
Beijing, China

Augusto Lima
School of Information Technology
and Engineering
University of Ottawa
Ottawa, Ontario, Canada

Chuang Lin
Department of Computer Science
and Technology
Tsinghua University
Beijing, China

Zhongxuan Liu
France Telecom R&D Beijing
Beijing, China

Florian Michahelles
Department of Management, Technology,
and Economics
Eidgenössische Technische Hochschule
Zurich, Switzerland

Ali Miri
School of Information Technology
and Engineering

and

Department of Mathematics and Statistics
University of Ottawa
Ottawa, Ontario, Canada

Bartolomeo Montrucchio
Dipartimento di Automatica e Informatica
Politecnico di Torino
Torino, Italy

Aristides Mpitziopoulos
Department of Cultural Technology
and Communication
University of Aegean
Lesvos, Greece

Monica Nevins
Department of Mathematics and Statistics
University of Ottawa
Ottawa, Ontario, Canada

Ilker Onat
School of Information Technology
and Engineering
University of Ottawa
Ottawa, Ontario, Canada

Goran Pantelić
Network Security Technology
Belgrade, Serbia

Grammati Pantziou
Department of Informatics
Technological Educational Institution
of Athens
Athens, Greece

Pedro Peris-Lopez
Computer Science Department
Carlos III University of Madrid
Madrid, Spain

Maurizio Rebaudengo
Dipartimento di Automatica e Informatica
Politecnico di Torino
Torino, Italy

Arturo Ribagorda
Computer Science Department
Carlos III University of Madrid
Madrid, Spain

Gabriel Robins
Department of Computer Science
School of Engineering and Applied Science
University of Virginia
Charlottesville, Virginia

Erwing R. Sanchez
Dipartimento di Automatica e Informatica
Politecnico di Torino
Torino, Italy

Raymond Sbrusch
Division of Computing and Mathematics
University of Houston–Clear Lake
Houston, Texas

Xuemin (Sherman) Shen
Department of Electrical and Computer
Engineering
University of Waterloo
Waterloo, Ontario, Canada

Minghui Shi
Department of Electrical and Computer
Engineering
University of Waterloo
Waterloo, Ontario, Canada

Andrea Soppera
British Telecommunications plc
Martlesham Heath
Ipswich, United Kingdom

Violeta Tomašević
School of Applied Informatics
Singidunum University
Belgrade, Serbia

Thijs Veugen
TNO Information and Communication Technology
Delft, the Netherlands

and

Department of Mediamatics
Faculty of Electrical Engineering, Mathematics, and Computer Science (EEMCS)
Delft University of Technology
Delft, the Netherlands

Qinghua Wang
Department of Information Technology and Media
Mid Sweden University
Sundsvall, Sweden

T. Andrew Yang
Division of Computing and Mathematics
University of Houston–Clear Lake
Houston, Texas

Tingting Zhang
Department of Information Technology and Media
Mid Sweden University
Sundsvall, Sweden

Zhibin Zhou
Computer Science and Engineering Department
Arizona State University
Tempe, Arizona

Part I

Security in RFID

1 Multi-Tag RFID Systems

Leonid Bolotnyy and Gabriel Robins

CONTENTS

Radio-frequency identification (RFID) is a promising technology for automated object identification that does not require line of sight, and accurate object identification is the primary objective of RFID. However, many factors such as object occlusions, metal/liquid opaqueness, and environmental conditions (e.g., radio noise) impede object detection, thus degrading the overall availability, reliability, and dependability of RFID systems. For example, a recent major study by Wal-Mart has shown that object detection probability can be as low as 66 percent. To improve the accuracy of object identification, we propose the tagging of objects with multiple tags. We show that this strategy dramatically improves the efficacy of RFID systems, even in the face of (radiopaque) metals and liquids, radio noise, and other interfering factors. We define different types of multi-tags and examine their benefits using analytics, simulations, and experiments with commercial RFID equipment. We investigate the effects of multi-tags on anticollision algorithms, and develop several techniques that enable multi-tags to enhance RFID security. We suggest new promising applications of multi-tags, ranging from improving patient safety to preventing illegal deforestation. We analyze the economics of multi-tag RFID systems and argue that the benefits of multi-tags can substantially outweigh the costs in many current applications, and that this trend will become even more pronounced in the future.

1.1 INTRODUCTION

Bar code scanners require a line of sight to the bar codes, and they usually have to be close to the objects being identified. Moreover, bar codes are scanned one at a time, and bar code scanners (or the bar codes themselves) must physically move between successive reads. This mechanical process limits the bar-code read rate to at most a few bar codes per second. On the other hand, RFID readers can read hundreds of tags per second and they do not require line of sight, thus allowing for fast automation of the reading process, and therefore making RFID-based identification very appealing commercially. However, as the identification process is automated, we must ensure the successful reading of all the tags within the readers' field to detect all objects.

Object detection is impeded by ubiquitous background radio noise. Moreover, metals and liquids reflect or absorb radio signals, further degrading the readers' ability to achieve accurate and complete tag identification. Missed items, even at a relatively low rate of 1 percent, can result in large financial losses for businesses with low profit margins that rely on RFID-enabled automatic checkout stations. This situation is real and serious, because milk, water, juices, and canned/metal-foil-wrapped (i.e., Faraday caged) goods are commonly stocked in markets. Experiments by Wal-Mart in 2005 showed 90 percent tag detection at case level, 95 percent tag detection on conveyor belts, and only 66 percent detection rate of individual items inside fully loaded pallets [1].

A report by the Defense Logistics Agency [2] showed that only 3 percent of the tags attached to objects moving through the Global Transportation Network (GTN) did not reach the destination (165 single-tagged objects were tracked in this study). However, the same report shows that only 20 percent of the tags were recorded in the GTN at every checkpoint, and at one of the checkpoints fewer than 2 percent of tags of one particular type were detected. In addition, some of the tags were registered on arrival, but not on departure. As a result of these low object detection rates, accurate real-time tracking of objects moving through the GTN network was not possible. This report underscores the unreliability of object detection using a single RFID tag per object.

Cardinal Health, a multi-billion-dollar healthcare company, conducted RFID trials in 2006 which showed mixed results [3]. Several product lines were automatically tagged, programmed, and later tracked. The company reported that only 94.8 percent/97.7 percent of tags were encoded correctly. The accuracy of product tracking varied widely from ~8 to 100 percent, depending on the product, the tracking location, and the tracking stage. Most product detection rates were in the low-80 percent to mid-90 percent range. These results show the inadequacy of standard RFID solutions for healthcare applications.

In addition to ambient radio noise, environmental conditions such as temperature and humidity can also adversely affect the success of object detection [4]. Moreover, objects moving at high speeds

can have significantly reduced detection rates. The number of objects stacked together, variation in tag receptivity (even among tags from the same manufactured batch), and tag aging (and degradation in general) can diminish the object detection probabilities as well. From the security standpoint, objects tagged with a single tag are easier to steal (a simple metal foil placed over the tag can block detection). In addition, RFID systems used in healthcare pose a special dependability challenge, because RFID system deployment will directly affect patients' welfare.

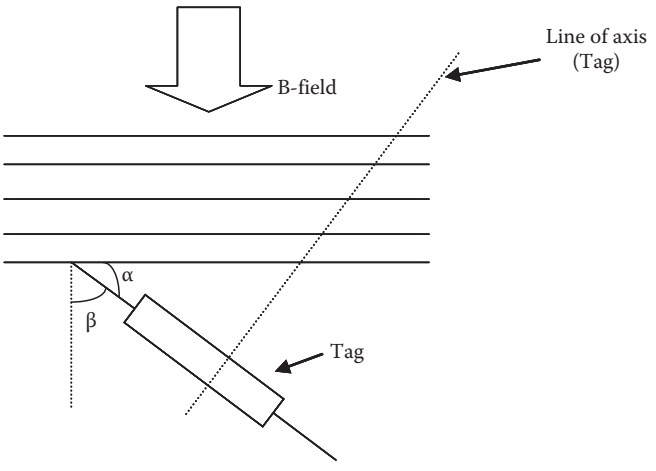
To address the problems discussed above, we propose attaching multiple RFID tags to each object, as opposed to using only a single tag per object [5]. Multi-tags will greatly improve object detection probabilities and increase reader–multi-tag communication distances, even in the presence of metallics, liquids, radio noise, and adverse environmental conditions. Multi-tags will greatly benefit theft deterrence and prevention applications, as well as dependable computing applications such as healthcare, where higher reliability and safety are required. All these benefits can be achieved at a reasonable cost, as we discuss below.

1.2 MULTI-TAG APPROACH

We base our analysis of multi-tags on the expected angle of incidence of the radio signal from the reader to the tag. We perform the analysis for inductive coupling as well as for far-field propagation. In the case of inductive coupling, Figure 1.1 depicts the angle α of the tag relative to the perpendicular direction of the signal transmitted from the reader, and gives the formula of the voltage induced in the tag by the received signal [6]. We analyze the expected voltage in one tag, as well as in ensembles of two, three, and four identical tags, assuming a fixed frequency, signal strength, and antenna geometry (i.e., loop area and number of antenna coil turns). In other words, we focus on the parameter that induces many of the benefits of multi-tags, namely the expected incidence angle of the arriving signal.

We define the angle β to be the angle between the tag and the direction of the arriving signal (rather than focusing on the angle between the tag and the perpendicular orientation of the tag to the B-field). We therefore replace cos(α) with sin(β) in the voltage equation in Figure 1.1. Our goal is to maximize sin(β) in the voltage equation to maximize the induced voltage and thus the strength of the received signal. Also, because power ∼ voltage^2 on board a tag, we obtain power ∼ sin^2(β).

Similarly, for far-field propagation, the power induced in the antenna by the signal is proportional to the gain of the antenna, which in turn is proportional to Poynting's vector $p = E \times H$ where E is the instantaneous electric field intensity and H is the instantaneous magnetic field intensity. We



$V_0 = 2\pi fNSB_0 \cos \alpha$

where

f is the frequency of the arrival signal

N is the number of turns of coil in the loop

S is the area in the loop (m^2)

B_0 is the strength of the arrival signal

α is the angle of the arrival signal

FIGURE 1.1 Reader-induced voltage on board a tag.

also have $E \sim \sin(\beta)$ and $H \sim \sin(\beta)$. So, we obtain power $\sim \sin^2(\beta)$ [7–9]. Therefore, to improve object detection for both inductive coupling and far-field propagation, we seek to bring the expected incidence angle β closer to 90°.

Besides improvements in expected power generated on board a tag, multi-tags improve object detection because even if one tag is occluded/damaged, another tag may still be detectable. In our theoretical analysis of improvements in object detection using multi-tags, we ignore environmental conditions (e.g., radio noise), object occlusions, presence of metals and liquids in the vicinity of an object, number of objects stacked together, etc. We will explore the effect of detection impeding factors in our extensive experimental studies discussed in Section 1.3.

1.2.1 Optimal Placement of Multi-Tags

The first question is how to orient the tags relative to each other to maximize the expected angle of incidence of the radio wave with respect to one of the tag antennas. In our analysis, we assume a uniform distribution for the direction of the arriving signal. Indeed, in many RFID applications the orientation of a tag's antenna to the arriving signal can be arbitrary (e.g., products in a shopping cart, cell phone in a pocket). In the case of a single tag, the tag can be positioned arbitrarily, because its orientation would not affect the expected (uniformly distributed) signal arrival angle. For two tags, it is optimal to position them perpendicular to one another in the x–y and x–z planes. Similarly, for three tags, tags should be positioned pair-wise perpendicularly in the x–y, x–z, and y–z planes. For four tags, it turns out that to maximize the expected signal incidence angle to at least one of the tags, it is best to position them parallel to the faces of a tetrahedron, a platonic solid.*

To validate our conjecture of optimal multi-tag placement for two and three tags, we computed the expected largest grazing angle of the radio signal to one of the tags analytically and using a simulation. The optimal placement of four tags was validated using simulations only, due to the considerable complexity of the corresponding analytical expressions. We first compute the expected largest grazing angle for two tags. Let α be the angle between two tags. Without loss of generality, let $0 \leq \alpha \leq \frac{\pi}{2}$. Then the average grazing angle ξ is

$$\xi = \frac{180}{\pi} \cdot \frac{1}{2\pi} \int_0^{2\pi} \int_0^{\frac{\pi}{2}} \text{Max}[\Delta_1, |\Delta_2|] \sin(\phi) d\theta \, d\phi$$

where

$\Delta_1 = \frac{\pi}{2} - \phi$

$\Delta_2 = \text{Arcsin}[\sin(\alpha)\sin(\theta)\sin(\phi) + \cos(\alpha)\cos(\phi)]$ [10]

To determine the optimal positioning of two tags, we want to maximize ξ subject to constraint that $0 \leq \alpha \leq \frac{\pi}{2}$. We performed computations of ξ using numerical integration in MATHEMATICA. The computations showed monotonic increase in ξ as the angle α increases from 0° to 90°. Therefore, when two tags are perpendicular to each other the expected largest grazing angle to one of the tags is maximal and equals ~47.98°. We can use the above ξ equation for two planes to compute the expected grazing angle for one plane by setting $\alpha = 0$. We obtain the following:

$$\xi = \frac{180}{\pi} \cdot \frac{1}{2\pi} \int_0^{2\pi} \int_0^{\frac{\pi}{2}} \left(\frac{\pi}{2} - \phi\right) \sin(\phi) d\theta \, d\phi \approx 32.7^\circ$$

* For five or more tags, it becomes more complicated to analytically determine the optimal relative positioning of the tags, except for specific special cases, such as for $N = 6$ where the tags should ideally be placed parallel to the faces of a dodecahedron, and $N = 10$ where the tags should be parallel to the faces of an icosahedron.

We performed similar computations for three tags. Let α be the angle between the first tag and the second tag. Let α_1 and α_2 be angles between tag 1/tag 3 and tag 2/tag 3, respectively. We obtain an almost identical expected angle formula as for two tags, except that additional coefficient are present in the body of the integral:

$$\xi = \frac{180}{\pi} \cdot \frac{1}{2\pi} \int_0^{2\pi} \int_0^{\frac{\pi}{2}} \text{Max}[\Delta_1, |\Delta_2|, |\Delta_3|] \sin(\phi) d\theta \, d\phi$$

where

$\Delta_1 = \frac{\pi}{2} - \phi$
$\Delta_2 = \text{Arcsin}[\sin(\alpha)\sin(\theta)\sin(\phi) + \cos(\alpha)\cos(\phi)]$
$\Delta_3 = \text{Arcsin}[x \cdot \cos(\theta)\sin(\phi) + y \cdot \sin(\theta)\sin(\phi) + z \cdot \cos(\phi)]$
$z = \cos(\alpha_1)$
$y = \dfrac{\cos(\alpha_2) - \cos(\alpha)\cos(\alpha_1)}{\sin(\alpha)}$
$x = \sqrt{1 - y^2 - z^2}$

Note, the above average angle ξ equation contains singularities, as it is not defined for some geometrically impossible (α_1, α_2) pairs [10]. The average angle ξ equation for three tags is much more complicated than the equation for two tags, and we computed the equation using numerical methods in MATHEMATICA for only select values of inter-tag angles α, α_1, α_2. The expected grazing angle values were computed extensively for all valid discrete (1°–90°) inter-tag angles using the simulation, which we describe below. The values computed using the simulation agreed closely with the values computed using MATHEMATICA, giving us confidence in the correctness of the formulas. The simulation showed that the optimal positioning of three tags is the mutually perpendicular positioning, resulting in the expected largest grazing angle $\sim$58.11°.

To corroborate our analytical computations of the largest average grazing angle, we developed a software simulator that computes the expected grazing angle for an arbitrary number of tags. The simulator enumerates all possible multi-tag orientations and for each orientation it calculates the average value of the maximum angle to any tag over many randomly generated simulated signals. The result of the simulation is the largest of the average maximum angles over all possible multi-tag positions. The simulator also records average maximum grazing angles for all orientations for future comparison with analytical computations.

To calculate the expected angle of incidence for a given multi-tag positioning, our simulator generates a random uniformly distributed point on the surface of a sphere [11]. This point determines the direction of a random uniformly distributed radio signal relative to the origin, and calculates the angle to every tag in the multi-tag ensemble, while recording the largest of these angles. For one- and two-tag ensembles our simulation generates 10 million such random trials and averages the induced maximum angles. For three-tag ensembles, it generates 1 million random trials, and for four tags, it generates 100,000 trials. The runtime of the simulator is $\Theta(k \cdot n^{2m-1})$ where k is the number of random reader signals, n is the number of possible angles between tags, and m is the number of tags (size of multi-tag ensemble), $m \geq 1$. Some of our simulations ran for several weeks on a single machine. Also, we ran week-long decomposed parallel computations on a cluster of 64 dual-processor Alpha PCs through portable batch system job scheduling software.

The results obtained from the analytical computations agree with the experimental results for one, two, and three tags at many points within a reasonably small error bound. We show the close match between the analytical and simulation computations for two tags in Figure 1.2. Similar results, although with smaller precision (due to fewer random trials) were obtained for three tags. The near-identical analytical and simulation results raise our confidence level in the correctness of the average angle computations. Accurate computations for one, two, and three tags allowed us to use only

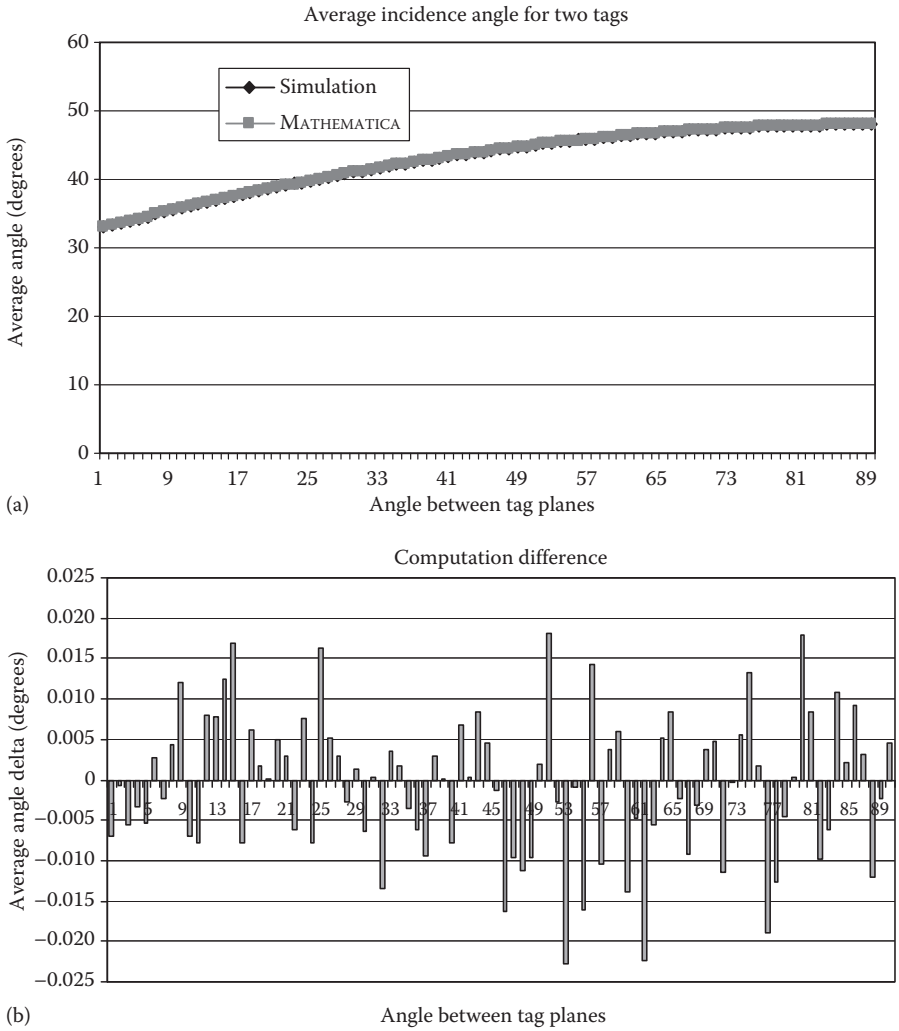


FIGURE 1.2 Accuracy of angle computation for two tags. Analytical and simulation computations are in tight agreement with at most several hundredth of a degree difference. (a) Comparison of analytical and simulation computations. (b) Computational error.

the simulator to compute the average angle for a larger tag ensemble (i.e., four tags), because the complex geometries involved make it intractable to analytically compute this quantity. For four tags, the average maximum grazing angle is ∼61.86°. Figure 1.3 shows the simulation results of the expected largest incidence angle for one-, two-, three-, and four-tag configurations.

We note that there is a two-digit increase in the expected angle as we move from one tag to two tags, and also as we go from two tags to three tags, but only a 3° improvement as we move from three tags to four tags. This suggests that adding an extra tag or two may be beneficial for the purpose of increasing the induced voltage (and thus improving the communication range), but using four or more tags will not garner substantial additional benefit in that respect. Nevertheless, even though the benefit of having more than three tags per object to increase the reader–tag communication range may be relatively small, there are other benefits to using more than three tags. For example, if an alternate benefit of multi-tags (e.g., theft prevention or human safety) is the primary goal, we may still benefit

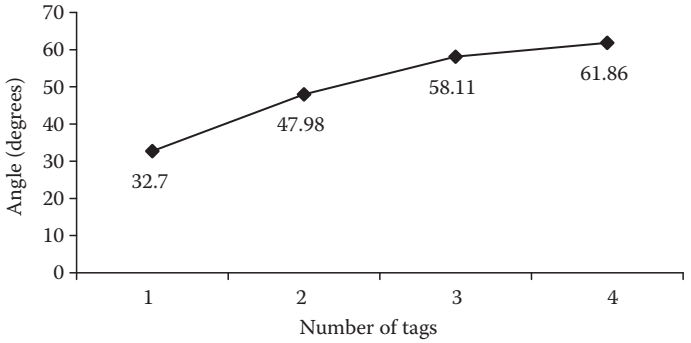


FIGURE 1.3 Expected largest reader signal's angle to any tag.

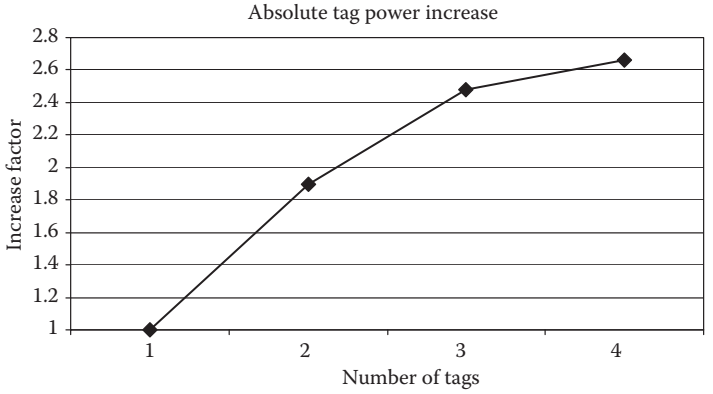


FIGURE 1.4 Absolute tag power increase for various number of tags per object.

from using more than three tags per object (and we can achieve further detection improvements by optimizing the tags' positioning).

Having computed the expected incidence angle improvements using multi-tags, we can determine the absolute and relative tag power gains for various multi-tag ensembles. Recalling that power $\sim \sin^2(\beta)$, Figure 1.4 shows the expected improvements in tag power. An increase in the expected tag power boosts the expected reader-to-tag communication distance. Figure 1.5 depicts the expected communication range increase for inductive coupling technologies as the number of tags is increased, and also for far-field propagation scenarios. These values were computed based on the relation of the distance between a reader and a tag, and the tag power generated by the reader. For backscattering technology, the effective communication distance varies as $\sim\sqrt{\text{power}}$; for inductive coupling, the maximum communication distance varies as $\sim\sqrt[6]{\text{power}}$ [12].

Our incidence angle-based analysis assumes that the signal can come from any direction with equal likelihood, which is realistic for many applications (e.g., goods randomly piled inside a shopping cart, cell phone arbitrarily placed inside a pocket). However, for some applications where the position/orientation of the object is known in advance or may only span a narrow range of possibilities, the optimal positioning of the tags may be different from the assumption-free ones suggested above. Similarly, the number of tags may vary among objects, to further optimize overall detection. Also, in our analysis of optimal multi-tag positioning we considered tag orientations only. However, to further improve objects detection, multi-tags should be spaced apart to reduce the likelihood of multiple tags being occluded simultaneously.

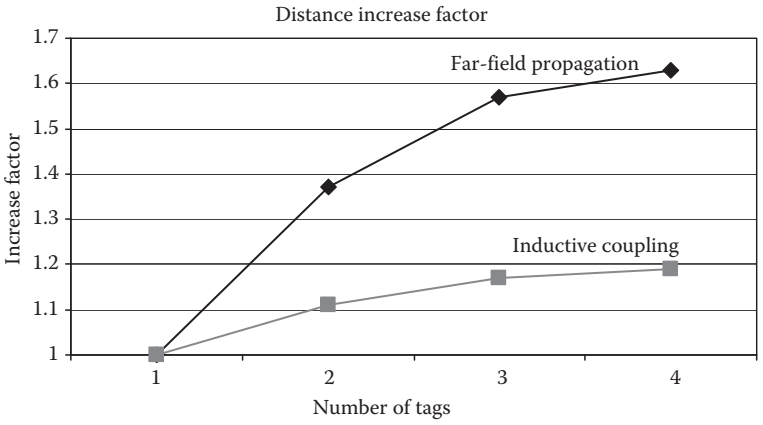


FIGURE 1.5 Expected factor of communication range increase for inductive coupling and far-field propagation as a function of the number of tags per object.

1.3 EXPERIMENTAL EQUIPMENT AND SETUP

To validate our analytical and simulation studies, we conducted an extensive experimental evaluation of multi-tags. Our experiments were performed using commercial FCC-compliant equipment (Figure 1.6), namely ultrahigh frequency (UHF) readers manufactured by Alien Technology (model ALR-9800, four antennas, multi-protocol, 915 MHz) and ThingMagic (model Mercury 4). We utilized sets of linear and circular reader antennas from Alien Technology, and circular reader antennas from ThingMagic. A single Alien Technology reader antenna can either broadcast or receive signals, whereas the more versatile ThingMagic antenna can both send and receive signals. We used several types of tags from UPM Raflatac, the world's leading RFID tag manufacturer. In particular, we picked unipolar (dipole) UPM Rafsec UHF "Impinj 34 × 54 ETSI/FCC" tags and bipolar (quadrupole) UPM Rafsec UHF "Impinj 70 × 70 ETSI/FCC" tags for our experiments.

We performed the experiments in an otherwise empty room to minimize radio interference and signal reflection anomalies. We placed multiple tags on a diverse set of 20 solid nonmetallic objects*

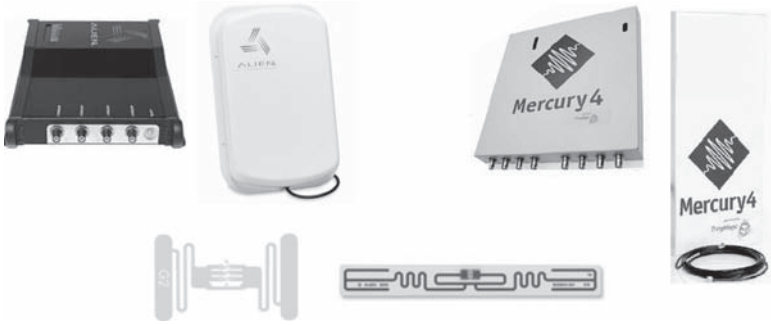


FIGURE 1.6 Multi-tag experimental equipment: Alien Technology Corporation reader and antenna (top left), ThingMagic reader and antenna (top right), UPM Rafsec and Alien Technology Corporation tag samples (bottom row).

* Solid nonmetallic multi-tagged objects included soap bars, cereal boxes, paper plates, plastic boxes, packaged foods, clothing items, etc.

using four tags per object, and a set of 20 metal and liquid-containing objects* using three tags per object. We positioned tags perpendicular to each other whenever possible, and spread the tags as far apart in space across an object as possible, to minimize tag occlusions by other tags or objects. The experiments with solid nonmetallic objects used sets of both unipolar and bipolar tags. The experiments containing metallic and liquid objects were performed only with unipolar UPM Rafsec UHF "Impinj 34 × 54 ETSI/FCC" tags.

We positioned Alien Technology reader antennas side-by-side in pairs, with each pair consisting of a sending and a receiving antenna. Each pair of antennas was equidistant to the center of a plastic bag containing objects, placed 20.5 in. above the floor, and aligned perpendicularly toward the center of the bag. We allowed sufficient time for the reader to read all the tags within its range by performing many tag reads and maintaining adequate time-outs between reads to make sure that the effects of the environmental noise were minimized. We performed our experiments for linear as well as for circular antennas using seven different power levels ranging from 25.6 to 31.6 dBm, in increments of 1 dBm.

In a separate set of experiments, circular ThingMagic antennas were equidistant and perpendicular to the bag containing the objects, located 33 in. above the floor, in the rectangular "gate" formation. Each ThingMagic antenna was both sending and receiving signals. As with the Alien Technology hardware, we allowed sufficient reader time for object identification. We randomly (re)shuffled the tagged objects multiple times to change the tags' spatial orientations with respect to the reader's antennas, to improve the statistical significance of the results (the values reported in the tables and graphs below are averages over all random object shufflings). We also varied the power emitted by the antennas, keeping in mind that the communication distance is proportional to $\sqrt{\text{power}}$.

We will mostly describe our experiments involving the Alien Technology hardware, because this equipment allowed us to collect data for both circular and linear antennas. Linear antennas have smaller angular coverage than circular (omnidirectional) antennas in exchange for greater signal strength in the specific direction. In the discussions and graphs below, we will implicitly assume that the Alien Technology equipment was used in each experiment, unless explicitly stated that the ThingMagic hardware was used instead. Similarly, all the experiments discussed in Section 1.4 have used the unipolar UPM Rafsec UHF tags "Impinj 34 × 54 ETSI/FCC," unless explicitly stated that bipolar tags were used.

1.4 EXPERIMENTAL RESULTS

1.4.1 Linear Antennas

Our experiments show that multi-tags considerably improve object detection probabilities for linear antennas. The detection probabilities for different numbers of tags per object, different numbers of reader antennas, and various reader power levels are summarized in Table 1.1. This table shows that switching from one to two tags per object produces a high double-digit increase in tag detection probability, and a low double-digit increase when moving from two to three tags, but only single-digit increase from three to four tags. These results corroborate our theoretical expectations [13].

Figure 1.7a graphically shows the increase in object detection probability for each object (the objects are sorted along the x-axis according to their detection probabilities). Again, we observe significant separations between the first three curves. In Figure 1.7b, we compare object detection improvements between two tags per object versus two reader antennas. From this data we can see a

* The multi-tagged metallic and liquid objects included cans of tomato sauce, canned vegetables, canned and bottled soda, bottled water, etc.

TABLE 1.1
Detailed Statistics Showing the Average Detection Probability for Linear Antenna(s) as a Function of the Power Level for Different Antenna Configurations and for Different Numbers of Tags Per Object

	Antenna Pair #1				Antenna Pair #2				Antenna Pairs #1 and #2			
	1 Tag	2 Tags	3 Tags	4 Tags	1 Tag	2 Tags	3 Tags	4 Tags	1 Tag	2 Tags	3 Tags	4 Tags
Power: 31.6 dBm	0.5800	0.7930	0.8945	0.9385	0.5715	0.7970	0.9010	0.9570	0.6495	0.8450	0.9300	0.9695
Power: 30.6 dBm	0.5280	0.7500	0.8575	0.9070	0.4730	0.6980	0.8210	0.8950	0.5890	0.7970	0.8930	0.9380
Power: 29.6 dBm	0.4645	0.6895	0.8110	0.8760	0.4220	0.6545	0.7925	0.8885	0.5370	0.7555	0.8635	0.9195
Power: 28.6 dBm	0.4140	0.6360	0.7645	0.8390	0.4350	0.6615	0.7920	0.8695	0.4920	0.7155	0.8295	0.8880
Power: 27.6 dBm	0.3425	0.5435	0.6770	0.7645	0.3765	0.5940	0.7340	0.8200	0.4380	0.6620	0.7880	0.8565
Power: 26.6 dBm	0.3275	0.5345	0.6740	0.7695	0.3235	0.5255	0.6635	0.7580	0.3985	0.6195	0.7540	0.8380
Power: 25.6 dBm	0.2575	0.4410	0.5790	0.6895	0.2785	0.4615	0.5825	0.6580	0.3430	0.5565	0.6975	0.7880

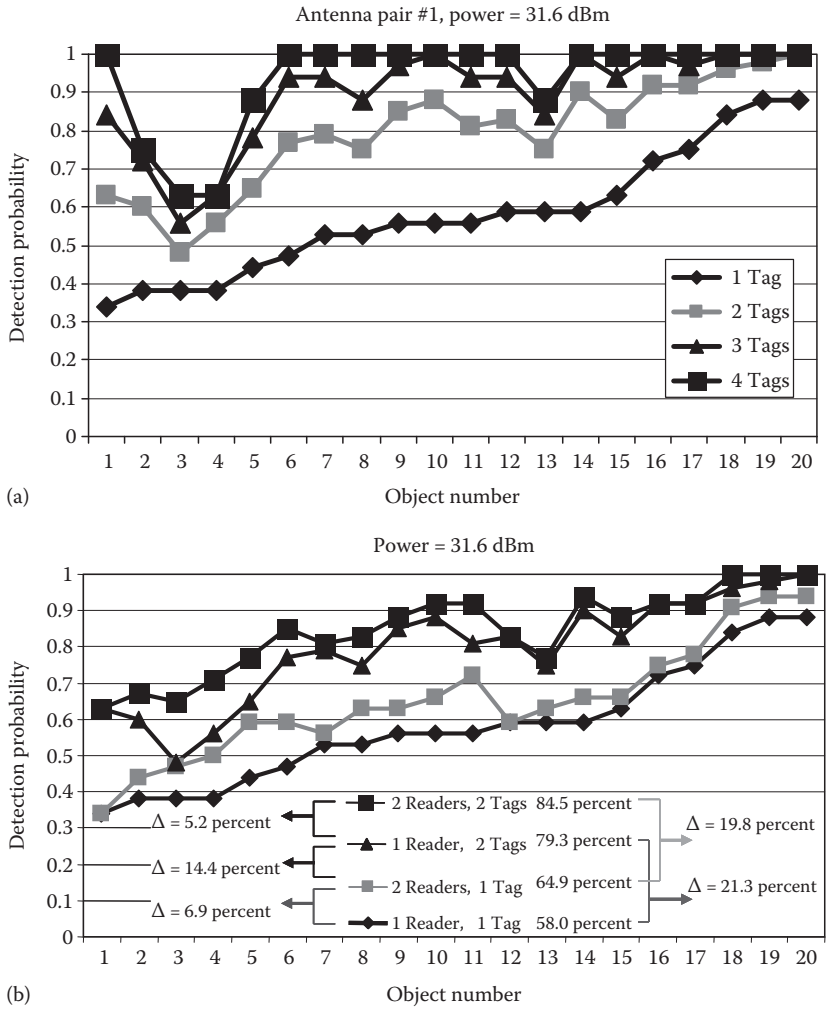


FIGURE 1.7 (a) Average object detection probability improvements for linear antennas as the number of tags per object increases. (b) Comparisons of multi-tags with multiple readers for linear antennas. Note that attaching multiple tags to an object yields higher average object detection probabilities than adding more readers. Objects are sorted based on single-tag detection probability.

dramatic double-digit improvement from adding a second tag to each object, and only a low single-digit improvement from adding a second reader, yielding almost a factor of 4 improvement in object detection probability using multi-tags as compared to multiple readers.

1.4.2 Circular Antennas

As with linear antennas, experiments with circular antennas show a dramatic double-digit average improvement in object detection as the number of tags per object increases. However, the detection probabilities for circular antennas are higher than for linear ones, because the orientation of objects with respect to the reader antennas varies widely. From the comparisons of different numbers of multi-tags and multiple readers (Figure 1.8), we can see that for circular antennas the advantage of adding a tag is on par with that of adding a reader. We also observed that the average object detection probabilities decrease more rapidly for circular than for linear antennas, as a function of decreasing antenna power [10].

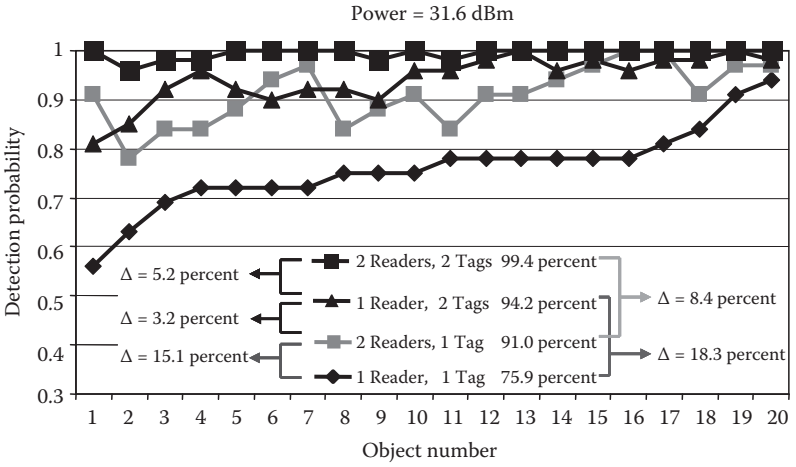


FIGURE 1.8 Comparing multi-tags with multiple readers for circular antennas. Attaching multiple tags to an object produces higher object detection probability than adding more readers. Objects are sorted based on single-tag detection probability.

1.5 IMPORTANCE OF TAG ORIENTATION

In our analytical analysis of multi-tags [13], we determined that (two or three) multi-tags should be oriented perpendicular to each other to obtain the most benefits in object detection. We experimentally confirm this claim by varying multi-tags orientation, collecting tag identification data, and calculating object detection probabilities for different multi-tag orientations. Then, we analyze these data and draw appropriate conclusions. We performed experiments with unipolar tags (UPM Rafsec UHF tag Impinj 34 × 54 ETSI/FCC) whose tag-plane orientation matters, and with bipolar tags (UPM Rafsec UHF tag Impinj 70 × 70 ETSI/FCC) whose tag-plane orientation has no effect on tag detection.

With unipolar tags, we ran experiments comparing differently oriented pairs of tags. One orientation which we call *180-same* refers to two tags positioned on the same plane and having identical orientation. The second orientation *180-diff* refers to two tags positioned on the same plane, but one of the tags is rotated 90° relative to the orientation of the other tag. The third orientation *90-same* refers to two tags having identical orientation, but positioned on perpendicular planes. Finally, the forth tag orientation *90-diff* refers to two tags positioned on perpendicular planes with one tag rotated 90° relative to the other tag. In our experiments we compared these four different tag orientations, and the results are presented in Figure 1.9a. The results show that tags perpendicular to each other yield a higher probability of detecting at least one of them than tags that have identical orientation. In addition, to increase detection probability, it is better to position tags on perpendicular planes, rather than to place all the tags in the same plane.

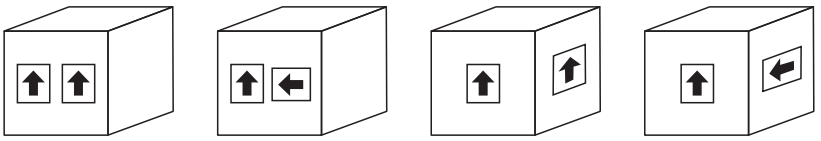
With bipolar tags we compared two possible tag orientations—180, where tags are positioned on parallel planes, and 90, where tags are positioned on perpendicular planes. These are the only possibilities because tag orientations within the plane have no effect on (ideal) bipolar tag detection. The results of the experiments shown in Figure 1.9b demonstrate no difference between tag orientations for omnidirectional/circular antennas, but a drastic advantage for perpendicular 90 tags over parallel 180 tags for directional/linear antennas. These results show that multi-tags improve object detection not only because they increase the total antenna size per object and decrease the probability of antenna occlusions but also because the expected grazing angle between the signal from the reader and one of the tags increases, which in turn raises the expected power on board one of the tags. These findings confirm our theoretical expectations.

	Circular		Linear	
	1 Tag	2 Tags	1 Tag	2 Tags
180-same		0.5500		0.3700
180-diff	0.4784	0.7454	0.3311	0.5272
90-same		0.6727		0.5272
90-diff		0.8000		0.6363

(a)

	Circular			Linear		
	1 Tag	2 Tags	3 Tags	1 Tag	2 Tags	3 Tags
180	0.75	1	1	0.53	0.57	0.70
90		0.93	1		0.97	1

(b)



(c)

FIGURE 1.9 The two tables comparing object detection probabilities for unipolar and bipolar tags for different multi-tag orientations. The results show the significance of perpendicular multi-tag orientation, especially for directional/linear antennas. In Figure 1.9a, *180-same* refers to identically oriented tags positioned on parallel planes; *180-diff* refers to perpendicularly oriented tags positioned on parallel planes; *90-same* refers to identically oriented tags positioned on perpendicular planes; *90-diff* refers to perpendicularly oriented tags positioned on perpendicular planes. In Figure 1.9b, 180 refers to tags positioned on parallel planes; 90 refers to tags positioned on perpendicular planes.

1.6 CONTROLLING EXPERIMENTAL VARIABLES

It is important in RF experiments to carefully isolate and control the variables to ensure the accuracy of the results. In our multi-tag experiments, we controlled the effects of radio noise, reader variability, tag variability, the number and type of reader antennas, reader power level, and the distance from the reader antennas to the objects. To control the effect of ambient radio noise, we ran our experiments multiple times, sometimes even across multiple days to ensure that statistical properties of the data are stable. To accurately calculate improvements in object detection with multi-tags, we allowed sufficient time for the reader to read the tags. The reader parameters were carefully selected to ensure that all tags within a reader's detectability range were read. To ensure that our results are independent of the particular reader and antenna manufacturer/brand, we ran our experiments with readers and antennas from two different manufacturers. In all of our experiments, we used consistent tag types and ensured that tag variability does not affect our experiments. We will discuss tag variability further in Section 1.6.1. The reader and identical reader antennas were carefully selected and objects were placed on a rotating platform at a fixed distance from the reader. The reader power levels were carefully controlled via a parameter in the software driver.

1.6.1 TAG VARIABILITY

To determine tag properties and control tag variability, we performed multiple tag variability tests. It is widely believed that RFID tags with different chip manufacturers and antenna geometries have different detectability/receptivity properties [14]. The importance of tag receptivity and its use as a tag performance metric is addressed in Ref. [15]. Similarly, no two chips are truly identical due

to inherent very-large-scale integration (VLSI) manufacturing variations [16]. Indeed, we found differences in tag detectability among tags of the same type, even among ones coming from the very same tag roll. In fact, these inherent tag receptivity differences were surprisingly high, with up to an order-of-magnitude difference in detectability between the "best" and "worst" tags. These findings provide yet another incentive for deploying multi-tags to ensure consistent object detection.

In our tag variability experiments, we used a ThingMagic reader, one circular ThingMagic antenna, and "UPM Rafsec UHF tag Impinj 34 × 54 ETSI/FCC" tags. Tags were elevated 26 in. from the floor, and positioned perpendicular to the antenna at a distance of 59.5 in. from the antenna center. The reader power level was set to 31.6 dBm. Each tag was read 200 times and the number of successful reads was recorded. We paused for 50 ms between reads to allow tags sufficient time to lose power and initialize their state. The reader was allotted 10 ms to read a tag. In this way, we computed the detectability/receptivity of 75 seemingly identical tags. To ensure data consistency, each experiment was performed twice and repeated the next day with the tags rotated 180°.

The smallest number of successful reads out of 200 was 8 and the largest was 91. The average was 43.44 and the standard deviation was 23.92. The Pearson product–moment correlation coefficient between two reads of each tag on the same day was 0.99 and the correlation between reads across two days was 0.98. Figure 1.10b shows the distribution of the number of successful tag reads, and Figure 1.10a compares the number of successful reads for each tag across the two sets of experiments conducted on consecutive days. To magnify the visual spread between tags, we show the number of successful tag reads out of 400 by summing the detectability across the two runs of each day. Similarly, high tag detectability variations were found in other UPM Rafsec tag types.

1.6.2 Reader Variability

To ensure that our results are not dependent on the reader/antenna manufacturers, we repeated our experiments using ThingMagic readers and ThingMagic circular antennas.* Because the tag detection algorithms used by ThingMagic and their implementations are different from those of Alien Technology, and because ThingMagic antennas are much bigger than those by Alien Technology, the detection probabilities we obtained differed between these two systems. However, the percentage improvements of multi-tags versus single-tagged objects were similar for both systems, supporting our hypothesis that the percentage improvements in object detection using multi-tags is mostly independent from the specific equipment used. Table 1.2 shows the statistics of object detection improvements using circular ThingMagic antennas for a different number of tag ensembles per object. In addition to providing the second set of data, the ThingMagic equipment enabled the collection of data for three and four antennas, whereas the Alien Technology readers work with only one and two antennas.

1.7 OBJECT DETECTION IN THE PRESENCE OF METALS AND LIQUIDS

So far we have discussed multi-tags experiments with only solid nonmetallic objects [17]. In some practical scenarios, however, the items to be identified can contain mixtures of nonmetallic objects, as well as metallic and liquid materials, making reliable object identification more problematic. It is more difficult to detect metallics and liquids because they tend to interfere with and occlude radio signals, thus preventing readers from receiving accurately decodable tag responses [18]. Metallic and liquid objects can also occlude other nonmetallic objects and thus interfere with the detection of these as well.

When metals and liquids are present, the detection probabilities for solid and nonmetallic objects decrease due to radio interference from the metallics and liquids. In our experiments, we observed a 4–10 percent decrease in the detection probability of solid objects, depending on the antenna type and the number of tags per object, as compared to situations where no liquids or metallics are

* Experimental results similar to ours using equipment from Symbol Technologies (now Motorola, Inc.) were reported [19].

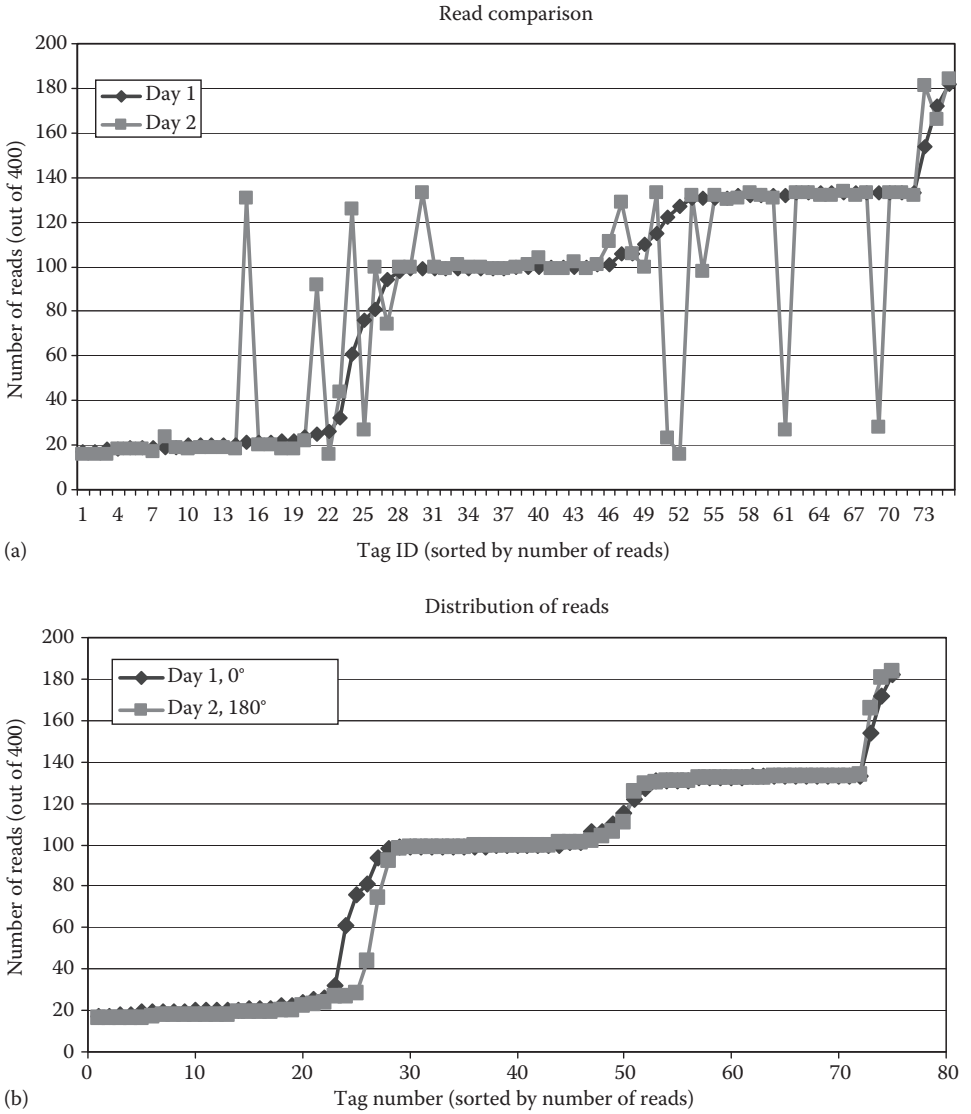


FIGURE 1.10 Characterization of tag detectability/receptivity. (a) Comparison of the number of successful reads per tag across two days. The tags are sorted based on the number of successful reads to better illustrate the data. (b) Distribution of successful tag reads across two days and two tag orientations. The number of successful reads shown is out of a total of 400 attempted. We observe a significant separation between several "clusters" of tag performance levels.

present. Figure 1.11 shows the average object detection probability for solid nonmetallic objects for circular reader antennas. In the graph, the top curve represents the detection probabilities of solid nonmetallic objects when metallics and liquids are absent, and the bottom curve represents the detection probabilities of solid nonmetallic objects when metallics and liquids are present.

To detect metallic and liquid objects in our experiments, we had to considerably reduce the distance from the objects to the readers to ensure that tags are actually detectable at that range. Specifically, we reduced the approximate reader-to-tag distance to 32 in., from the 55 in. range used for solid and nonmetallic objects. In addition, we had to operate readers at high power levels only. To avoid using special tags that are specifically designed for metals and liquids, and be able to compare

TABLE 1.2
Detection Probability Statistics for Circular ThingMagic Antennas as a Function of the Power Level for Different Antenna Configurations and for a Different Number of Tags Per Object

	1 Antenna				2 Antennas			
	1 Tag	2 Tags	3 Tags	4 Tags	1 Tag	2 Tags	3 Tags	4 Tags
Power: 31.6 dBm	0.6528	0.8511	0.9291	0.9662	0.8335	0.9580	0.9874	0.9979
Power: 30.6 dBm	0.5668	0.7775	0.8761	0.9257	0.7567	0.9129	0.9537	0.9667
Power: 29.6 dBm	0.4813	0.6932	0.8033	0.8653	0.6755	0.8630	0.9233	0.9485
Power: 28.6 dBm	0.3818	0.5778	0.6960	0.7736	0.5614	0.7702	0.8588	0.9105
	3 Antennas				4 Antennas			
	1 Tag	2 Tags	3 Tags	4 Tags	1 Tag	2 Tags	3 Tags	4 Tags
Power: 31.6 dBm	0.8847	0.9782	0.9958	1	0.8910	0.9800	0.9970	1
Power: 30.6 dBm	0.8176	0.9442	0.9686	0.9750	0.8255	0.9465	0.9690	0.9750
Power: 29.6 dBm	0.7476	0.9100	0.9492	0.9615	0.7600	0.9160	0.9515	0.9630
Power: 28.6 dBm	0.6355	0.8323	0.9025	0.9400	0.6535	0.8450	0.9100	0.9445

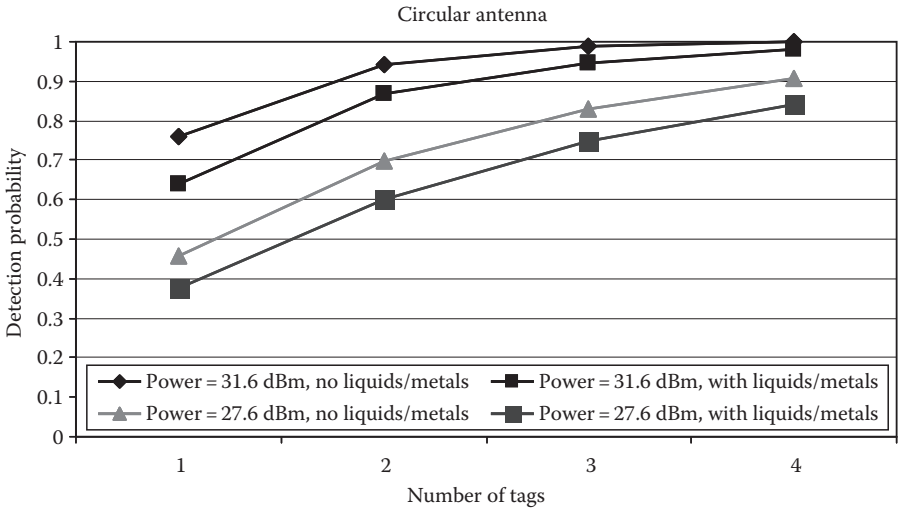


FIGURE 1.11 Comparison of average detection probabilities using circular antennas for solid nonmetallic objects when metallic/liquid objects are present and absent.

relative improvements of multi-tags for solid/nonmetallic objects with liquids and metallics, we used a few millimeter thin spacers between the objects and the tags. The space between the objects and the tags enabled bouncing radio signals to detect tags, yet kept the tags close enough to the metallic and liquid objects to retain the signal-interfering absorption and reflection characteristics of the liquids and metals.

Based on our experimental results, multi-tags are highly effective in improving object detection in the presence of metallics and liquids. We observed an almost linear improvement in metallic and liquid objects detection when the number of tags per object is increased, as compared to the rapidly increasing and then leveling detection probability curve for solid nonmetallic objects. Figure 1.12 shows detection probability for several power levels and antenna configurations. The results of separate experiments using the ThingMagic hardware show rapidly vanishing improvements in object

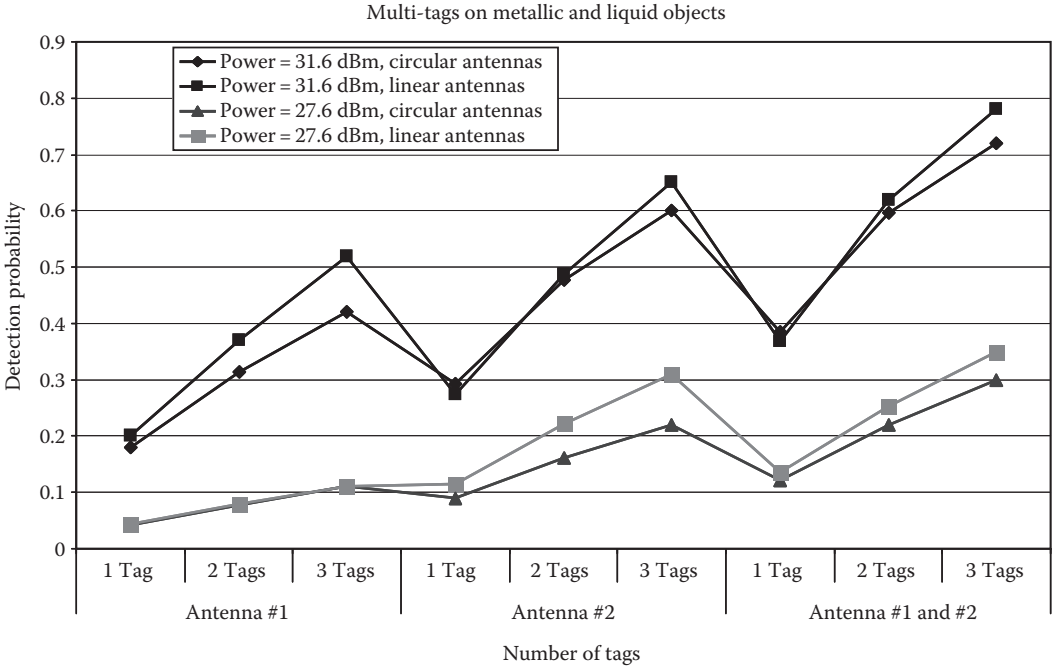


FIGURE 1.12 Comparison of average detection probabilities of metallic and liquid objects using one and two linear and circular antennas for various power levels.

detection probabilities as the number of antennas increases, yet an almost linear improvement in object detection probabilities as the number of tags per object is increased [10].

1.8 EFFECT OF OBJECT QUANTITY ON DETECTION

Aside from environmental conditions such as temperature, humidity, radio noise, and the presence of metallics and liquids in the objects' vicinity, the mere number of objects stacked together affects the average detection probability of an object. This occurs because the objects to be identified act as radio signal occluders, shielding other objects' tags from the readers. To better understand the effect of the number of objects on the average object detection probability, we conducted several experiments. The results of these experiments confirmed our expectations and revealed interesting patterns that we describe next.

We performed two back-to-back experiments to determine the effect of the number of objects on the average object detection probability. In these experiments, we used circular ThingMagic antennas and unipolar tags. In the first experiment, we grouped 15 solid nonmetallic and 15 metallic and liquid objects and determined the average object detection probabilities for liquids and metallics, and separately for solid, nonmetallic objects. In the second experiment, we grouped 20 solid nonmetallic and 20 liquid metallic objects, and again determined the average object detection probabilities. To ensure that the reader has sufficient time to detect all reader-visible tags in both experiments, we allocated 3 s for the reader to detect tags in the 15/15 experiment and (proportionally) 4 s for the 20/20 experiment. The detection probability statistics were calculated for various numbers of tags per object, as well as different numbers of reader antennas. For accurate comparison, in calculating the statistics in the second experiment, we used a subset of 15 solid nonmetallic and 15 liquid metallic objects that matched the objects in the first experiment.

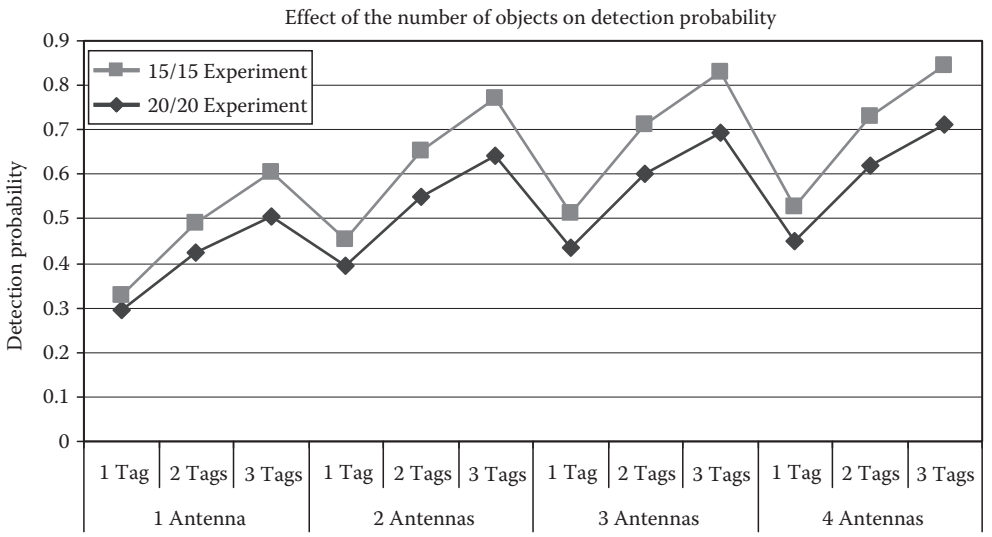


FIGURE 1.13 Effect of the number of objects on the average object detection probability. In the 15/15 experiment, we used 15 metallic and liquid objects, and 15 solid nonmetallic objects. Similarly, in the 20/20 experiment, we used 20 metallic and liquid objects, and 20 solid nonmetallic objects.

We compared the average object detection probabilities between two experiments, varying the number of tags per object and the number of reader antennas. Figure 1.13 shows the results of this comparison for metallic and liquid objects. Observe that the average detection probability of an object in a 15/15 experiment is greater than in a 20/20 experiment, as expected (because higher numbers of objects increase the likelihood of occlusions). The difference is more dramatic and vivid for metallic and liquid objects than for solid nonmetallic ones because the reader is operating at a high power level to detect metallic and liquid objects.

Note that the difference in object detection probabilities between the two experiments is greater when more tags are attached to an object, and when multiple readers are used for object identification. This occurs due to an overall improvement in object detection when multi-tags and multiple readers are used. These experiments clearly illustrate that multi-tags have a more positive influence than multiple readers on detection probabilities, especially in the presence of metallics and liquids, and when identifying larger groups of objects.

1.9 EFFECT OF MULTI-TAGS ON ANTICOLLISION ALGORITHMS

Anticollision algorithms enable a reader to uniquely identify tags while minimizing the number of tag broadcasting collisions (i.e., simultaneous interfering transmissions by the tags). Multi-tags have no effect on two variants of Binary Tree-Walking [8,20], and may at most double/triple the total read time for double/triple-tags over single tag for Slotted Aloha [8] and for Randomized Tree-Walking [21–23]. Our theoretical and experimental study of multi-tags addressed how multi-tags improve object detection. It is worth noting, however, that because not all tags are detected, the time required to identify all reader-visible tags is considerably less than double (or triple) the time needed to identify single-tagged objects by some anticollision protocols.

In particular, from our experiments we observed that 25–75 percent of all tags on solid/nonmetallic objects are detected with one reader antenna, depending on its type and power level. The percentages are much lower for metallic and liquid objects. Therefore, attaching two tags to each object may not add any significant overall time delay for object identification. Moreover, current RFID technology can read hundreds of tags per second, making the increase in the number of tags

insignificant, even in real-time systems. Finally, in many scenarios the benefits of successfully identifying all the objects certainly justifies a modest increase in identification time. Based on the above observations, RFID system designers should select an appropriate anticollision algorithm based on the number of objects that may have to be identified near-simultaneously, the number of tags attached to each object, and the expected objects' velocities (if the objects to be identified are moving).

1.10 MULTI-TAGS AS SECURITY ENHANCERS

1.10.1 Chaffing and Winnowing

Multi-tags can enhance RFID security using the idea of "chaffing and winnowing" [24]. Chaffing creates messages with phony message authentication codes (MACs), and winnowing filters fake messages by comparing the MAC received along with the message against the MAC computed by the recipient. The achieved confidentiality can be made arbitrarily strong with smaller packet sizes. Sending chaff probabilistically, or controlling the amount of chaff sent will hide the real number of tags in the reader's interrogation zone [23]. This relatively low-cost technique is especially useful in preventing adversaries from performing accurate inventorization. For example, a business may want to perform rapid covert inventorization of a competitor, relying on RFID tagged inventory, and thus gain valuable information about a competitor's business practices. Prevention of unauthorized inventorization is a very interesting problem that merits future research.

1.10.2 Preventing Side-Channel Attacks

Multi-tags can prevent certain side-channel attacks (e.g., "power analysis" attacks). An adversary can use power analysis attack to learn the kill password* of an electronic product code (EPC) tag, as demonstrated by Oren and Shamir in Ref. [25]. They showed that when an EPC compliant tag receives a kill password from the reader one bit at a time, the tag's power operation changes, allowing an adversary to detect power spikes when the tag receives an invalid bit. In a multi-tag scenario, one tag can counterbalance the power budget of the other tag by operating in an "opposite" mode, thus preventing simple power analysis, and consequently preventing the discovery of a kill password by an adversary.

1.10.3 Splitting ID among Multi-Tags

Another technique to prevent accurate adversarial inventorization is the splitting of the tag ID/data into several parts, and distribute these parts among multi-tags. The multi-tags can transmit the data to the readers at different frequencies using code division multiple access, making it difficult for an adversary to reconstruct the complete signal (tag ID/data). This technique was used by the British during World War II to prevent the Germans from jamming Allied transmissions [26]. Note that the data splitting technique is unlikely to prevent adversarial tracking on its own because the tag's data is sent in the clear, but in conjunction with privacy preserving techniques it can be a powerful security mechanism. Splitting the data between tags may lower the overall cost of the system.

1.11 APPLICATIONS OF MULTI-TAGS

Multi-tags can be deployed in a variety of useful applications and serve many purposes. They can be used for specific tasks such as determining the location and orientation of objects, as well as ensuring system reliability, availability, and even safety. In addition, multi-tags can be a considerable deterrent to illegal activities such as theft and forgery, and they can enhance RFID security and privacy. For example, multi-tags can speed up the execution of some algorithms through parallel computation. Below, we give examples of scenarios and systems where multi-tags can be effective. These examples

* When a tag receives the correct kill password from a reader, it stops responding to future reader queries.

do not cover all possible applications; rather, they serve mainly to illustrate the wide range of uses and applications of multi-tags.

1.11.1 Reliability

There are many RFID applications where system reliability is critical. For example, in a store scenario, checkout RFID readers should reliably detect all items purchased by the consumer. Missed items, even at a relatively low rate of 1 percent, can incur huge losses to a typical low-profit-margin business, thus significantly affecting the store's bottom line. Also, objects moving through a supply chain should be detected reliably to enable accurate real-time inventory control and early theft detection. In general, in most applications where goods change hands or objects move through an RFID checkpoint, all objects should be detected and identified accurately. Multi-tags attached to objects will greatly increase objects' detection probabilities at a reasonable cost.

1.11.2 Availability

One example where multi-tags can improve system availability is in "yoking-proof" scenarios, where a potentially adversarial reader communicates with a group of tags and generates a proof that the tags were identified near-simultaneously [27,28]. The constructed proof is later verified by an off-line verifier. The integrity of the system hinges on the tags of all objects being detectable by the reader when required, because otherwise no valid proof can be created, even by an honest reader. The problem is exacerbated because of the tight timing constraints of the protocol, and the inherent variations in tag receptivity [17]. In such "yoking-proof" scenarios, multi-tags can be attached to each object, thus greatly increasing the probability of at least one tag per object being detectable. Note that here multi-tags may need to be physically connected to each other, so that they can consistently share their states with each other to prevent the possible forgery of a yoking proof. Another example of an application where availability is important is the real-time tracking of critical household or business objects such as remote controls, car keys, firearms, and important documents, among others.

1.11.3 Safety

Another, perhaps unexpected, area where multi-tags can be of great benefit is safety. Specifically, multi-tags can be used in healthcare to track medical instruments (e.g., gauze sponges). For example, surgical sponges, among other foreign objects, are sometimes left inside humans during operations, causing highly undesirable consequences that adversely affect the patients. Recent medical studies [29] have shown surprisingly good results in detecting RFID-equipped surgical gauze sponges during operations. However, to accurately detect all the sponges requires very careful and precise positionings of the reader. If the distance between the reader and the tags is increased even slightly, the tags may go undetected and thus the object may be inadvertently left inside the patient. In addition, the sponges may be located amid bodily fluids, further decreasing the detection probabilities. Finally, the tags on the sponges may break or malfunction, causing readers to miss tags, which may result in serious human injury. Attaching multi-tags to surgical sponges will greatly increase the probability of all sponges being detected and accounted for, which would translate into improved patient safety and reduced hospital liability.

1.11.4 Object Location

The location of a multi-tagged object can be more accurately determined than that of a single-tagged one. Well-known location triangulation methods can be utilized to determine the position of each tag, thus reducing the error in computing a multi-tagged object's location coordinates. A carefully engineered multi-tag RFID system can be used to determine not only an object's position but also its spatial orientation [30]. Directional antennas and orientation-sensitive RFID tags can be deployed

to make such a system highly effective. Creating a working prototype of such a system and applying it in real-world scenarios is an interesting area for future research.

1.11.5 Packaging

Many RFID tag types are delivered to the customer on a continuous paper roll, and the customer later programs the tags with unique IDs. We envision that tags will soon be cheap enough to embed into, e.g., adhesive packaging tape used to wrap packages and containers, thus simplifying the multi-tagging of boxed objects, and enabling automatic tag diversity and orientation selection to greatly improve object detection at negligible cost. With higher tag ubiquity and the multi-tagging of objects, the testing of RFID tags will be obviated, because even a low tag production yield will enable the overall system to function properly. The acceptability of lower tag manufacturing yields will further reduce the production costs, while ensuring high object detection probabilities as well as improved dependability and reliability of RFID systems.

1.11.6 Theft Prevention

Another useful set of applications of multi-tags is in theft prevention. Increasing the number of tags attached to (or embedded in) an object will make it much more difficult for a thief to shield or remove all of the tags, thereby increasing the probability of him getting caught. For example, one intriguing application of this could be the prevention of illegal deforestation* by embedding tags in the trunks of living trees [13]. Because tags are very cheap compared to the cost of lumber (especially for rare or legally protected trees such as Redwoods), the economics of such applications are financially viable. When logs are shipped and sold, they can be scanned for tags whose presence will determine the origin of the wood (and possibly convey other useful information, such as weather and environmental statistics tracked over the tree's lifetime). It would be prohibitively expensive for illegal loggers to detect and remove all of the tags from a given tree trunk, thus substantially increasing the cost and risk of illegal deforestation, at a relatively low cost to the protection agencies.

The attachment of the radio antenna(s) to the silicon chip, and tag packaging itself incur the majority of the cost in RFID tag manufacturing [31]. However, if we use multi-tags for theft prevention as described above, we neither need to package the tags nor be particularly precise or careful when attaching antenna(s) to chips. The mere large number of tags per object will guarantee that enough tags are still detectable, and will thus deter theft. The simpler process of producing unpackaged tags will considerably streamline the tag manufacturing process and consequently reduce their cost. In addition, in such scenarios, manufacturing yields are no longer required to remain high, and tag testing steps may be skipped as well, further contributing to significant tag cost reductions. We discuss the economics of multi-tag RFID in more detail in the next section.

1.11.7 Tagging Bulk Materials

Cheap redundant multi-tags can be embedded into bulk materials (e.g., fertilizers, explosives, chemicals, propellants, crude oil, etc.) to prevent their unintended acquisition, transportation, and possible misuse. If tags are embedded into certain bulk materials at a reasonably small proportion to the size/quantity/weight of a substance, they will not adversely affect the normal use of these materials (e.g., crude oil can be tagged at the rate of ten multi-tags per barrel, and these tags can be removed during the final stages of the refinement process). If required, the tags can have limited lifespans or even be (bio)degradable. The RFID tagging of fertilizers/explosives can help law enforcement agencies trace the producer or buyer. The tagging of bulk materials can also directly prevent criminals/terrorists from causing damage by enabling law enforcement agencies to detect the presence of dangerous substances in proximity (or ominously en route) to sensitive locations or particular sites of interest, hopefully before an illegal act transpires.

* Illegal deforestation is not a hypothetical problem (e.g., see a recent news article in Ref. [32]).

1.12 ECONOMICS OF MULTI-TAGS

Based on RFID trials by corporations and government agencies (see Section 1.1), and our experimental results [17], it is clear that object detection probabilities are far from perfect, even when multiple readers/antennas are used. Multi-tags, potentially in conjunction with multiple readers, can help address the object detection problem. The cost of RFID tags in 2007 is around 8¢ each, making the multi-tagging of high-cost items viable today. In addition, the cost of tags is decreasing at an exponential rate following Moore's law, and this trend will enable the cost-effective tagging of even low-cost objects in the near future. Also, the cost of RFID tags is decreasing substantially faster than the cost of RFID readers, due to improving manufacturing yields and an economy of scale driven by massive deployments. Moreover, this price gap is expected to continue to widen due to the increasing demand for cheap RFID tags. The anticipated future omnipresence and ubiquity of RFID tags is expected to eventually reduce the cost of RFID tags into the subpenny level.

1.12.1 Costs and Benefits of Multi-Tags

The cost of passive RFID tags has been decreasing rapidly over the last decade. From 2001 to 2006, the cost of passive tags has speedily dropped from $1.15 to $0.08 a piece, when at least 1 million units were purchased [33–35]. Based on this historical data, we predict that tags will cost $0.06 by the end of 2007, and 5¢ in 2008. A 5¢ price point for tags was considered the threshold for supporting a strong business case for item-level tagging [36], and now this target price is just around the corner. Based on the efforts of some companies and researchers working on RFID tag technology [31,37], we believe that ~1 penny tags will become a reality around the year 2011. Eventually, tags will be printed directly onto objects and cost less than a penny to produce. This cost milestone will make RFID a truly ubiquitous and affordable technology. Figure 1.14 depicts the historical (and our projected) decreasing cost trends for tags.

When considering the cost of RFID tags or even the cost of an entire RFID system, it is critical to also analyze the benefits that RFID brings to an application. A complete business analysis of deploying RFID should be performed, because the benefit of deploying RFID in an application can considerably outweigh the cost, even at today's prices. Specifically, the business analyses of RFID systems should take into account the direct savings that RFID deployment will enable, such as higher employee productivity, automated business processes, workforce reductions, and the valuable information collected through RFID.

In supply chain management scenarios, the benefits of RFID deployment are tremendous. First, the merchandize can be tracked in real-time, allowing more efficient scheduling of operations. RFID may also allow reductions in the number of workers, because many currently manual processes can be automated. RFID can also prevent theft of goods, which are stolen predominantly by insiders. According to National Association for Shoplifting Prevention (NASP), insider thieves outnumber outsider thieves six to one [38,39]. It has been documented that over 1 percent of goods in retail

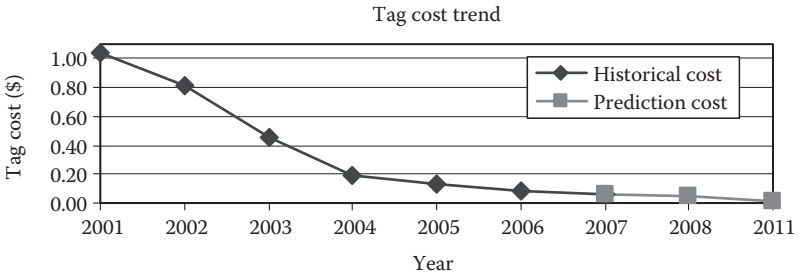


FIGURE 1.14 Cost trend of passive RFID tags over time, and our cost prediction for the future. The price per tag is based on the purchase of at least 1 million tags.

stores are stolen [39], and the real losses due to theft are likely to be much higher, as companies tend to underreport theft statistics. Multi-tag technology enables objects to be tracked more effectively, not only during transport or checkout but also during manufacturing and warehousing, which can significantly reduce theft rates and thereby increase profits.

1.12.2 Tag Manufacturing Yield Issues

Manufacturing yield is one of the main criteria that influence the cost of VLSI chips. This is because customers have to pay not only for the good chips delivered to them but also for the defective chips that never made it out of the fabrication facility, as well as for the labor-intensive separation of the good ones from the defective ones. For example, according to recent research by RFID vendors, as many as 30 percent of RFID chips are damaged during production when chips are attached to their antennas, and an additional 10–15 percent are damaged during the printing process [4].

Due to the redundancy built into our proposed multi-tag RFID systems, we can often ignore the manufacturing yield. Some manufactured RFID tags may be defective, while others may fail in the field, but if multiple tags are attached to each object, the probability that all the tags fail is still quite small. This considerably increases the overall reliability of a multi-tag RFID system, and also decreases the tag manufacturing costs (e.g., expensive manufacturing steps such as testing may be dispensed with).

The failure rate of deployed RFID tags in the field is estimated to be as high as 20 percent [40]. This large failure rate induces an additional cost pressure on RFID tag manufacturing, because individual tags must be made more reliable, or extensively tested after manufacturing. Even after packaging, tags may become defective. For example, 5 percent of the tags that we purchased for our experiments were marked by the manufacturer as defective; moreover, we discovered several additional inoperable tags during the tag programming phase of our experiments. As with the yield issue, multi-tags allow us to ignore damaged tags and statistically rely on the promise that enough multi-tags will remain operational to satisfy an application's requirements. This property of multi-tag systems helps to improve the overall reliability and cost of deployed multi-tag RFID systems.

1.12.3 RFID Demand Drivers

A strong driver of cost in RFID systems is the scope of the demand for this technology. With increases in demand, the number of produced RFID units will increase, which drives the amortized development costs down. However, many companies are hesitant to deploy RFID technology because the business case is not entirely clear or proven. This classic "chicken-and-egg" dilemma has inhibited the massive deployments of RFID systems so far. With improvements in RFID technology, the cost of RFID systems should decrease, creating a more convincing business case for companies and accelerating the demand for the technology, which will in turn reduce the amortized cost of RFID tags even further. The demand for RFID will be driven by many companies with a wide range of specializations and fields, led by major players such as Wal-Mart and DoD, and the desire to remain competitive in rapidly evolving marketplaces. Consequently, companies will experience mounting pressures to adopt RFID technology, and multi-tag-based strategies will help bootstrap undecided companies into this technology and help propel them into the RFID age.

1.12.4 Cost-Effective Tag Design Techniques

Overall tag cost can be reduced by developing better and cheaper tag components and assembling them in a more cost-effective manner. We give some practical examples of advanced memory design, antenna design, and assembly technologies to illustrate how technological developments drive down RFID costs. The cost of RFID tags can be reduced through innovative lower-cost memory design technologies. For example, the chip manufacturer Impinj, Inc., uses "self-adaptive silicon," which enables the low-cost reliable analog storage of bits in floating gates [41]. Another way to decrease the

tag cost is to speed up the tag manufacturing and packaging processes. For example, Alien Technology has developed fluidic self-assembly (FSA), which allows for the placement of a large number of very small components across the surface in a single operation, significantly speeding up tag assembly. This technology involves flowing tiny microchips in a special fluid over a base containing holes shaped to catch the chips [42]. In addition to designing antennas with improved receptivity and orientation, measures can be taken to lower antenna costs. For example, Symbol Technologies reduced the cost of antennas by manufacturing them out of aluminum rather than silver. The company also compressed antennas into small, low-powered inlay, thus reducing tag area and cost [43].

1.12.5 Summary of Multi-Tag Economics

RFID technology leverages Moore's law in the positive direction. RFID tags are getting both smaller and cheaper over time, resulting in a multiplicative corresponding reduction in tag cost. In addition, RFID tag yields are improving, further compounding the effect of these trends on cost reduction. Also, engineering and manufacturing tolerances for RFID chips are much larger than for high-end chips (e.g., RFID chips can operate at low clock speeds, extreme miniaturization is not a prominent problem in RFID production, etc.). Moreover, the VLSI manufacturing equipment for RFID tags does not have to be cutting edge, which reduces the cost pressure when constructing tag fabrication facilities. Rapidly increasing demand for RFID, along with cheaper manufacturing techniques and improving yields, is expected to rapidly bring the cost of RFID tags into the subpenny levels in the near future, making multi-tags ever more affordable. In short, multi-tags are clearly economically viable, and their benefits are bound to become even more dramatic over time.

1.13 CONCLUSION

There are many obstacles to reliable RFID-based object identification. Environmental conditions such as temperature, humidity, ambient radio noise, object quantities/geometries, etc. can significantly interfere with object detection and accurate identification. Dramatic variations in tag receptivity and detectability, even among tags of the same type and production batch, reduce the reliability of tag detection. The metals and liquids present in or around objects (or the environment) can reflect or absorb radio signals, thus preventing accurate signal decoding. In addition, objects density, concentration, and placement geometry can adversely influence object detection, thus affecting the availability, reliability, and even safety of an RFID system.

To significantly improve object detection, we proposed to attach multiple RFID tags (multi-tags) to each object. We defined different types of multi-tags. Through analytics, simulations, and experiments, we showed that multi-tags should be positioned perpendicular to each other whenever possible, and separated from each other to reduce chances of occlusion. Our experiments showed that multiple readers improve object detection only moderately, yet multi-tags provide much more dramatic gains in average object detection probability. We showed that multi-tags are very effective in dealing with radio noise, tag variability, and the presence of metallics and liquids among objects, as well as high object densities. We gave examples of numerous applications that could greatly benefit from multi-tags. We proposed several techniques to enhance RFID security using multi-tags. We analyzed the economics of multi-tags and argued that multi-tags are cost-effective even today for many cost-sensitive, safety-critical, and security-oriented applications. We predicted that multi-tags will become cost-justifiable for many more applications in the near future, as the cost of passive tags continues to rapidly drop. We also stressed the importance of careful RFID system design to ensure the desired operation and performance.

It is important to note that although multi-tags considerably improve object detection, especially in conjunction with multiple readers, they do not guarantee 100 percent object detection. Given the numerous obstacles to reliable object identification, it is very difficult to provide detection guarantees. In practical RFID deployments, the deployment site should be carefully analyzed for radio interfering phenomenon, allowing the system engineers to make appropriate design decisions. More research in

the areas of RFID chip and antenna design, as well as RF technology, is needed to further improve the reliability of RFID-tagged object detection.

Neglecting to carefully consider the benefits and costs of multi-tags in a specific deployment may result in financial loses, degraded overall system performance, and other unintended consequences. For example, improving object detection might unexpectedly aid thieves in locating valuable items, thus hurting object owners. Similarly, the overuse of multi-tags may create additional interferences in the operation of anticollision algorithms, thus degrading object detection. It is also possible that for some applications multi-tags are not economically viable because they may require unjustifiable investment in extra tags and equipment to optimize tag placement. In general, RFID deployments require careful planning and testing on a case-by-case basis.

In summary, we believe that multi-tag RFID technology promises many benefits to numerous applications, and will expedite reductions in tag manufacturing cost. This will positively tip the cost-benefit scale in favor of massive RFID deployments, and encourage many companies, organizations, and communities to join the age of ubiquitous RFID.

ACKNOWLEDGMENT

This research was supported by grant CNS-0716635 from the National Science Foundation.

REFERENCES

[1] IDTechEx. RFID progress at Wal-Mart. www.idtechex.com/products/en/articles/00000161.asp, October 2005.

[2] SRA International, Inc. Resolute ordinance movement evaluation. http://www.dla.mil/j-6/ait/Documents/Reports/Resolute_Ordinance_May2001.as%px, May 2001. Appendix F—GTN Tag History.

[3] Cardinal Health releases RFID pilot results. http://www.cardinal.com/content/news/11142006_91731.asp, November 2006. Cardinal Health, Dublin, OH.

[4] Gao. Key considerations related to federal implementation of radio frequency identification technology. http://www.gao.gov/new.items/d05849t.pdf, June 2005. Testimony before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security.

[5] L. Bolotnyy and G. Robins. Multi-tag rfid systems. *International Journal of Internet Protocol Technology, Special Issue on RFID: Technologies, Applications, and Trends*, 2(3/4):218–231, 2007.

[6] Y. Lee. RFID coil design. Technical Report AN678, Microchip Technology, Inc., Chandler, AZ, 1998. ww1.microchip.com/downloads/en/AppNotes/00678b.pdf.

[7] C. A. Balanis. *Antenna Theory Analysis and Design*. John Wiley & Sons, New York, 1997.

[8] K. Finkenzeller. *RFID Handbook*. John Wiley & Sons, West Sussex, England, 2003.

[9] T. Scharfeld. An analysis of the fundamental constraints on low cost passive radio-frequency identification system design. Master's thesis, MIT, Cambridge, MA, 2001.

[10] L. Bolotnyy. New directions in reliability, security and privacy in radio frequency identification systems. PhD thesis, University of Virginia, Charlottesville, VA, 2007.

[11] G. Marsaglia. Choosing a point from the surface of a sphere. *Annals of Mathematical Statistics*, 43(2):645–646, 1972.

[12] M. Reynolds. The physics of RFID, 2003. http://www.media.mit.edu/events/movies/video.php?id=rfid privacy-2003-11-15-1.

[13] L. Bolotnyy and G. Robins. Multi-tag radio frequency identification systems. In *Proceedings of the IEEE Workshop on Automatic Identification Advanced Technologies (Auto-ID)*, pp. 83–88, Buffalo, NY, October 2005.

[14] E. Schuster, T. Scharfeld, P. Kar, D. Brock, and S. Allen. Analyzing the rfid tag read rate issue. http://mitdatacenter.org/CutterITAdvisor.pdf, 2004.

[15] Impinj. Receptivity—A tag performance metric. www.impinj.com/files/MR_MZ_WP_00005_Tag Receptivity.pdf, December 2005.

[16] Y. Chen, A. B. Kahng, G. Robins, and A. Zelikovsky. Area fill synthesis for uniform layout density. *IEEE Transactions on Computer-Aided Design*, 21(10):1132–1147, 2002.

[17] L. Bolotnyy, S. Krize, and G. Robins. The practicality of multi-tag rfid systems. In *Proceedings of the International Workshop on RFID Technology—Concepts, Applications, Challenges (IWRT 2007)*, pp. 100–113, Madeira, Portugal, June 2007.

[18] L. Bolotnyy and G. Robins. The case for multi-tag rfid systems. In *International Conference on Wireless Algorithms, Systems and Applications (WASA)*, Chicago, IL, August 2007.
[19] A. Rahmati, L. Zhong, M. Hiltunen, and R. Jana. Reliability techniques for rfid-based object tracking applications. In *Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 113–118, Edinburgh, U.K., June 2007.
[20] A. Juels, R. Rivest, and M. Szedlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In V. Atluri (ed.), *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 103–111, Washington, DC, October 2003.
[21] Auto-ID Center. Draft Protocol Specification for a 900 MHz Class 0 Radio Frequency Identification Tag, 2003.
[22] L. Bolotnyy and G. Robins. Randomized pseudo-random function tree walking algorithm for secure radio-frequency identification. In *Proceedings of the IEEE Workshop on Automatic Identification Advanced Technologies (Auto-ID)*, pp. 43–48, Buffalo, NY, October 2005.
[23] S. Weis. Security and privacy in radio-frequency identification devices. Master's thesis, MIT, Cambridge, MA, May 2003.
[24] R. Rivest. Chaffing and winnowing: Confidentiality without encryption. *CryptoBytes*, 4(1):12–17, 1998.
[25] Y. Oren and A. Shamir. Power analysis of rfid tags, 2006. http://www.wisdom.weizmann.ac.il/~yossio/rfid/.
[26] D. Nolan. Internet technologies in a converged network environment. *NCS Technical Information Bulletin* 04-2, 2004.
[27] L. Bolotnyy and G. Robins. Generalized 'yoking proofs' for a group of radio frequency identification tags. In *International Conference on Mobile and Ubiquitous Systems (Mobiquitous)*, San Jose, CA, July 2006.
[28] A. Juels. "yoking-proofs" for RFID tags. In R. Sandhu and R. Thomas (Eds.), *International Workshop on Pervasive Computing and Communication Security*, pp. 138–143, Orlando, FL, March 2004.
[29] A. Macario, D. Morris, and S. Morris. Initial clinical evaluation of a handheld device for detecting retained surgical gauze sponges using radiofrequency identification technology. *Archives of Surgery*, 141:659–662, 2006.
[30] S. Hinske. Determining the position and orientation of multi-tagged objects using rfid technology. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*, pp. 377–381, White Plains, NY, March 2007.
[31] P. Peumans. Monolithic, low-cost rfid tags. http://peumans-pc.stanford.edu/research/monolithic-low-cost-rfid-tags, 2006. Project at Stanford Organic Electronics Lab.
[32] KIROTV.com. *3 Accused of Felling Old-Growth Trees*. http://www.kirotv.com/news/14210458/detail.html, September 2007.
[33] R. Moscatiello. Forecasting the unit cost of RFID tags. http://www.mountainviewsystems.net/Forecasting%20the%20Unit%20Cost%20of%20RFID%20Tags.pdf, July 2003.
[34] M. O'Connor. Alien drops tag price to 12.9 cents. *RFID Journal*. http://www.rfidjournal.com/article/articleview/1870/1/1/, September 2005.
[35] M. Roberti. A 5-cent breakthrough. *RFID Journal*. http://www.rfidjournal.com/article/articleview/2295/1/128/, May 2006.
[36] S. Sarma. Towards the five-cent tag. Technical Report MIT-AUTOID-WH-006, 2001. Auto-ID Labs.
[37] OrganicID, Inc. Printable, plastic RFID tags. In *Printed Electronics*, OrganicID, Inc., New Orleans, LA, December 2004.
[38] National Association for Shoplifting Prevention (NASP). Shoplifting statistics. www.shoplifting prevention.org.
[39] M. Vargas. Shoplifting and employee theft recovery up last year. http://retailindustry.about.com/od/lp/a/bl_hayes_theft.htm, 2005. From 17th Annual Retail Theft Survey by Jack L. Hayes International, Inc.
[40] *RFID Journal*. RFID system components and costs, 2005. http://www.rfidjournal.com/article/articleview/1336/3/129/.
[41] Impinj, Inc. Our technology. http://www.impinj.com/advantage/our-technology.aspx.
[42] FSA manufacturing. http://www.alientechnology.com/technology/fsa_manufacturing.php. Alien Technology, Inc., Morgan Hill, CA.
[43] Symbol Technologies. Symbol technologies launches portfolio of RFID generation 2 and specialty tag inlays, May 2006. http://news.thomasnet.com/companystory/484018.

2 Attacking RFID Systems

Pedro Peris-Lopez, Julio Cesar Hernandez-Castro,
Juan M. Estevez-Tapiador, and Arturo Ribagorda

CONTENTS

A great number of hackers end up working in the security departments of IT and telecommunications companies. In other words, the best way of making a system secure is knowing how it can be attacked. Radio-frequency identification (RFID) is no different from any other technology, so the possible attacks on it should be studied in depth. The extent of an attack can vary considerably; some attacks focus on a particular part of the system (e.g., the tag) whereas others target the whole system. Although there are references to such attacks in a number of publications, a rigorous study has not been made of the subject until now. We examine, in this chapter, the main threats to RFID security. First, we look at data and location privacy. Although these are the risks most often referred to in the literature, there are other equally important problems to consider too. RFID systems are made up of three main components (tag, reader, and back-end database), so we have grouped the threats according to the unit involved in the attack. First, we examine those related to tags and readers such as eavesdropping, cloning, replay, and relay attacks. Then we look at the threats to the back-end

database (e.g., object name service [ONS] attack, virus). By the end of this chapter (and with the opportunity to consult the extensive bibliography for further details), we hope the reader will have acquired a basic understanding of the principal security risks in RFID.

2.1 INTRODUCTION

2.1.1 Background

Press stories about radio-frequency identification (RFID) often give inaccurate descriptions of the possibilities that exist for abuse of this technology. They predict a world where all our possessions will have a unique identification tag: clothes, books, electronic items, medicines, etc. For example, an attacker outside your house equipped with a commercial reader would be able to draw up an inventory of all your possessions, and particular information such as your health and lifestyle could also be revealed. Also, it is said that this technology allows "Big Brother" to know when you are in public places (office, cinemas, stores, pubs, etc.), tracking all your movements and compromising your privacy in terms of your whereabouts (location).

RFID technology is a pervasive technology, perhaps one of the most pervasive in history. While security concerns about the possibility of abuse of this pervasive technology are legitimate, misinformation, and hysteria should be avoided. One should be aware that ways of collecting, storing, and analyzing vast amounts of information about consumers and citizens existed before the appearance of RFID technology. For example, we usually pay with credit cards, give our names and address for merchandizing, use cookies while surfing the Internet, etc.

In this chapter we give an overview of the risks and threats related to RFID technology, helping the reader to become better acquainted with this technology. Although the privacy issues are the main focus in literature [1–12], there are other risks that should be considered when a RFID system is designed.

2.1.2 Attack Objectives

The objectives of each attack can be very different. It is important to identify the potential targets to understand all the possible attacks. The target can be the complete system (i.e., disrupt the whole of a business system) or only a section of the entire system (i.e., a particular item).

A great number of information systems focus solely on protecting the transmitted data. However, when designing RFID systems, additional objectives, such as tracking or data manipulation should be considered. Imagine the following example in a store: an attacker modifies the tag content of an item reducing its price from 100 € to 9.90 €. This leads to a loss of 90 percent for the store. In this scenario, the data may be transmitted in secure form and the database has not been manipulated. However, fraud is carried out because part of the system has been manipulated. Therefore, to make a system secure, all of its components should be considered. Neglecting one component, whatever the security level of the remaining components, could compromise the security of the whole system.

The objectives of the attacks are very different. As we see in the above example, the attack may be perpetrated to steal or reduce the price of a single item, while other attacks could aim to prevent all sales at a store. An attacker may introduce corrupt information in the database to render it inoperative. Some attacks, such as the faraday cage or active jamming, are inherent in the wireless technology employed. Other attacks are focused on eliminating physical access control, and ignore the data. Other attacks even involve fraudulent border crossings, identity stealing from legitimate e-passports, etc.

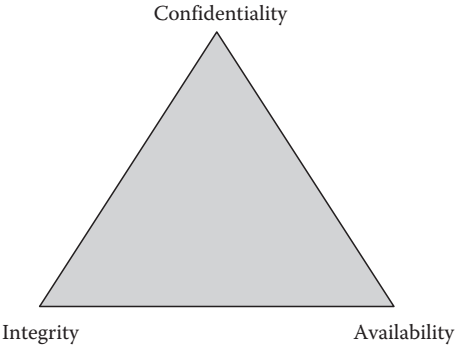


FIGURE 2.1 Three pillars of security: the CIA triad.

2.1.3 Security Needs

As any other mission-critical system, it is important to minimize the threats to the confidentiality, integrity, and availability (CIA) of data and computing resources. These three factors are often referred to as "The Big Three." Figure 2.1 illustrates the balance between these three factors.

However, not all systems need the same security level. For example, not all systems need 99.999 percent availability or require that its users be authenticated via retinal scans. Because of this, it is necessary to analyze and evaluate each system (sensitivity of the data, potential loss from incidents, criticality of the mission, etc.) to determine the CIA requirements. To give another example, the security requirements of tags used in e-passports should not equal those employed in the supply chain (i.e., tag compliant to EPC Class-1 Generation-2).

Confidentiality: The information is accessible only to those authorized for access. Privacy information, such as the static identifiers transmitted by tags, fits into the confidentiality dimension. Both users and companies consider this issue of utmost importance. Furthermore, RFID technology allows the tracking of items. From a user perspective, tracking should be avoided. However, companies may control the movements of materials in the supply chains, increasing the productivity of their processes.

Integrity: The assurance that the messages transmitted between two parties are not modified in transit. Additionally, some systems provide the authenticity of messages. The receipt is able to prove that a message was originated by the purported sender and is not a forgery (nonrepudiation). An example of this kind of attack is the spoofing attack.

Availability: System availability is whether (or how often) a system is available for use by its intended users. This factor will determine the performance and the scalability level of the system. Denial-of-service (DoS) attacks are usual threats for availability (i.e., active jamming of the radio channel or preventing the normal operation of vicinity tags by using some kind of blocker tag).

Each time a new technology is implanted, contingency plans for various points of failure should be designed. We recommend periodical security audits to review the security polices, procedures, and IT infrastructures. As has been frequently mentioned, RFID technology may be a replacement for bar-code technology. Nevertheless, new risk scenarios should be considered with its implantation. For example, consider the repercussions of a bar-code reader failing or an RFID reading going down. When a bar-code reader fails, an operator can manually enter the codes into the terminal and the system works, albeit with relatively slowness. On the other hand, if the RFID reader is processing high volumes of items and these items are moving at high speed, the consequences will be much worse. Security needs should therefore be considered a priority.

2.2 MAIN SECURITY CONCERNS

2.2.1 PRIVACY

No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks [13].

Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of individuals, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals [14].

Privacy has no definite boundaries and its meaning is not the same for different people. In general terms, it is the ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves.

The invasion of privacy by governments, corporations, or individuals is controlled by a country's laws, constitutions, or privacy laws. For example, taxation processes normally require detailed private information about earnings. The EU Directive 95/46/EC [14] on the protection of individuals with regard to the processing of personal data and the free movement of this, limits and regulates the collection of personal information. Additionally, Article 8 of the European Convention of Human Rights identifies the right to have private and family life respected. Within this framework, monitoring the use of e-mails, Internet, or phones in the workplace, without notifying employees or obtaining their consent can result in legal action.

RFID technology is a pervasive technology, and seems destined to become more and more so. As Weiser already predicted in 1991, one of the main problems that ubiquitous computing has to solve is privacy [15]. Leakage of information is a problem that occurs when data sent by tags reveals sensitive information about the labeled items. Products labeled with insecure tags reveal their memory contents when queried by readers. Usually, readers are not authenticated and tags answer in a transparent and indiscriminate way.

As an example of the threat this could pose, consider the pharmaceutical sector where tagged medication is planned for the immediate future. Imagine that when you leave the chemist's with a given drug—say an antidepressive or AIDS treatment, an attacker standing by the door equipped with a reader could find out what kind of medication you have just bought. In a similar scenario, thieves equipped with tag readers could search people, selecting those with multiple tagged bank bills to rob, and they would know how much they would earn with each robbery.

Advanced applications, where personal information is stored in the tags, have appeared recently. E-passports are a good example of this sort of application. As part of its U.S.-VISIT program, the U.S. government mandated the adoption of e-passports by the 27 nations in its Visa-Waiver Program. A combination of RFID technology and biometric technology is employed [7,16,17]. The RFID tags store the same information that is printed on its first page (name, date of birth, passport number, etc.) as well as biometric information (facial image). In phase-2 of the European e-passport project [18], the biometric data from two fingerprints, which is very sensitive information, will also be stored.

Several organizations like CASPIAN [19] and FOEBUD [20] are strongly against the massive deployment of RFID technology. They believe that RFID technology will lead to a significant loss of citizens' privacy. Some of CASPIAN's activities include successful boycott campaigns against important companies like Benetton [21,22], Tesco [23], and Gillette [24], to name but a few. Additionally, a book titled "*SPYCHIPS: How Major Corporations and Government Plan to Track your Every Move with RFID*" and published in 2005 [25], has contributed to promoting suspicion about RFID technology.

Another example of objection to RFID technology is the case of California State Senator Joe Simitian (Senate Bill 682), who planned to restrict the use of identification systems based on RFID technology: "The act would prohibit identity documents created, mandated, or issued by various

public entities from containing a contactless integrated circuit or other device that can broadcast personal information or enable personal information to be scanned remotely" [26]. Due to significant industry opposition, Bill 682 was stalled in the Assembly Appropriations Committee and an important missed deadline resulted in the expiry of the Bill. Legislative maneuvring allowed the resurrection of the case by means of Bill 768 [27]. This bill was finally vetoed by California Governor Arnold Schwarzenegger. In particular, Bill 768 proposed to

1. Criminalize the "skimming" of personal data from RFID-enable identification documents.
2. Implement specific provisions to ensure the security of data contained in such identification documents.
3. Impose a three-year moratorium on the use of RFID technology in certain types of government-issued identification documents.

In 2002, Garfinkel proposed a set of rights that should be upheld by any system that uses RFID technology [28]. Consumers should have:

1. Right to know whether products contain RFID tags.
2. Right to have RFID tags removed o deactivated when they purchase products.
3. Right to use RFID-enabled services without RFID tags.
4. Right to access an RFID tag's stored data.
5. Right to know when, where and why the tags are being read.

These rights are not necessarily considered as the basis for a new law, but as a framework for voluntary guidelines that companies wishing to deploy this technology may adopt publicly.

2.2.2 Tracking

Location information is a set of data describing an individual's location over a period of time [29]. The resolution of the system (time and localization) depends on the technology used to collect data.

Indeed, location privacy can be viewed as a particular type of privacy information [30]. A secondary effect of wireless communication is that information can be made public and collected. In a mobile phone context, the regions are divided up into cells. Each time a phone enters a new cell, the mobile is registered. Mobile phone operators record handset location information and supply it to third parties (i.e., police, the company that subscribed the localization service, etc.). Other techniques such as triangulation can be used to increase the precision of the system. The new localization services (i.e., third-generation mobile phones) allow an accuracy of a few meters by means of the incorporation of a global positioning system (GPS) receiver. In data network context, Wireless 802.11 Ethernet cards obtain connectivity by registering with access points which could be used to locate a network device.

RFID technology is not a high-tech bugging device. It does not possess GPS functionality or the ability to communicate with satellites. RFID tags do not have the storage and transmission capability for large quantities of information. An RFID system is normally composed of three components: tags, readers, and a back-end database. Readers are connected, using a secure channel, to the database. When a database is present in the system, tags might only transmit an identifier. This identifier is used as a index-search in the database to obtain all the information associated with the tag. Therefore, only people with access to the database can obtain the information about the labeled item.

Most of the time, tags provide the same identifier. Although an attacker cannot obtain the information about the tagged item, an association between the tag and its holder can easily be established. Even where individual tags only contain product codes rather than a unique serial number, tracking is still possible using an assembly of tags (constellations) [31]. To clarify the potential risks of tracking, some examples are given:

Wall-Mart: It is an American public corporation, currently one of the world's largest. It has concentrated on streamlining the supply chain, which is why it encourages all its suppliers to incorporate RFID technology in their supply chains. The substitution of bar codes by RFID tags allows an increase in the reading-rate of the pallets as they move along the conveyor belt. RFID readers can automatically scan these as they enter or leave the warehouse, saving time and improving product flow. Right now, RFID technology is used at pallet level. Individual packaging is the next logical step.

Individual product packaging: Imagine that your Tag Heuer bifocals possess a tag, and this tag stores a 96 bit static identifier, allowing an attacker to establish a link between the identifier and you. On association, an attacker could know when you passed through a given place, for example when you enter or leave your home, when you arrive at or leave your office, etc. Even worse, the attacker could locate several readers in your favorite mall. He could collect data over a long time (data, time, shop, etc.) acquiring a consumer profile of you. Finally, he could send you personalized advertising information depending on your shopping habits.

E-passports: Since October 2006, the United States required the adoption of e-passports by all the countries in its Visa-Waiver Program. The International Civil Aviation Organization (ICAO) standard specifies one mandatory cryptographic feature (passive authentication) and two optional cryptographic features (basic access control and active authentication). Passive authentication only demonstrates that tag content is authentic but it does not prove that the data container is secure. Basic authentication ensures that tag content can only be read by an authorized reader. Additionally, a session key is established, encrypting all the information exchanged between the tag and the reader. Active authentication is an anticloning feature, but it does not prevent unauthorized readings. Independent of the security mechanism used, tracking is possible. The electronic chip required by the ICAO must conform to ISO/IEC 14443 A/B already adopted in other applications [32,33]. The collision avoidance in ISO 14443 uses unique identifiers that allow readers to distinguish one tag from another [17]. However, this identifier will allow an attacker to unequivocally identify an e-passports's holder. One simple countermeasure is to generate a new random identifier each time the tag is read.

As has been shown, RFID technology is not the only one that permits the tracking of people (i.e., video surveillance, mobile phone, Wireless 802.11 Ethernet cards, GPS, etc.). Nevertheless, the equipment used to track people holding RFID tags is not very expensive. If we return to the example of tracking in a mall, we will understand one of the principal differences between RFID and other localization technologies. The great majority of malls have a video surveillance system. You can be filmed in all the supermarket sections in which you buy an item. Then, the information obtained by the system (images) has to be processed to obtain your consumer profile. However, if RFID technology was employed, data could be automatically collected without the need for subsequent data processing as in video systems.

2.3 TAGS AND READERS

2.3.1 Operating Frequencies and Reading Distances

RFID tags operate in four primary frequency bands [34]:

1. Low frequency (LF) (120–140 kHz)
2. High frequency (HF) (13.56 MHz)
3. Ultrahigh frequency (UHF) (860–960 MHz)
4. Super high frequency/microwave (μW) (2.45 GHz and above)

The characteristics of different frequencies are summarized in Table 2.1.

TABLE 2.1
Tag Frequencies and Reading Distances

Frequency Band	Frequency	Distance	Energy Transfer
Low (LF)	125 kHz	1–90 cm, typically around 45 cm	Inductive coupling
High (HF)	13.56 MHz	1–75 cm, typically under 40 cm	Inductive coupling
Ultrahigh (UHF)	865–868 MHz (Europe) 902–928 MHz (United States) 433 MHz (active tags)	Up to 9 m	Electromagnetic coupling
Microwave (μW)	2.45 GHz 5.8 GHz	Typically 0.3–0.9 m	Electromagnetic coupling

LF tags: These tags operate at 120–140 kHz. They are generally passive and use near-field inductive coupling. So they are suited for applications reading small amounts of data at relatively slow speeds and at short distances. Their read range varies from 1 to 90 cm, typically below 45 cm. LF tags do not support simultaneous tag reads. LF tags are relatively costly because they require a longer, more expensive copper antenna. They penetrate materials such as water, tissue, wood, and aluminum. Their common applications are in animal identification, automobile security, electronic article surveillance, commerce, and other areas.

HF tags: These tags operate at 13.56 MHz. They are typically passive and typically use inductive coupling. HF tags penetrate materials well, such as water, tissue, wood, aluminum, etc. Their data rates are higher than LF tags and their cost is lower due to the simple antenna design. Their read ranges varies from 1 to 75 cm, typically under 40 cm. HF tags are used in smart shelf, smart cards, libraries, baggage handling, and other applications.

UHF tags: UHF active and passive tags can operate at different frequencies. UHF active tags operate at 433 MHz, and UHF passive tags usually operate at 860–960 MHz. Generally, passive UHF tags are not very effective around metals and water. They perform well at distances greater than 90 cm. UHF passive tags usually reach about 9 m. UHF tags have good non-line-of-sight communication, a high data rate, and can store relatively large amounts of data.

Super high frequency/microwaves tags: These tags operate at frequencies of 2.45 GHz and above (also 5.8 GHz) and can be either active or passive. Their characteristics are similar to those of UHF tags. However, they have faster read rates and are less effective around metals and liquids than tags of lower frequencies. These tags can be smaller in size compared to LF, HF, and UHF tags and are used for electronic toll collection as well as for the tracking of shipping containers, trains, commercial vehicles, parking, etc. The read range varies from 0.3 to 0.9 m for passive tags and is very dependent on design. Active systems also use microwave frequency.

2.3.2 Eavesdropping

RFID technology operates through radio, so communication can be surreptitiously overheard. In Ref. [35], the possible distances at which an attacker can listen to the messages exchanged between a tag and a reader are categorized (see Figure 2.2).

Forward channel eavesdropping range: In the reader-to-tag channel (forward channel) the reader broadcasts a strong signal, allowing its monitoring from a long distance.

Backward channel eavesdropping range: The signal transmitted in the tag-to-reader (backward channel) is relatively weak, and may only be monitored in close proximity to the tag.

Operating range: The read ranges shown in Section 2.3.1 are the operating read range using sales-standard readers.

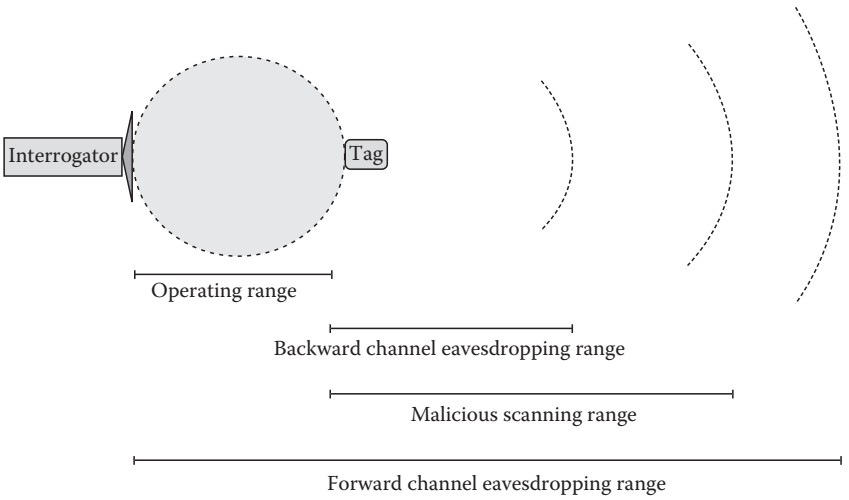


FIGURE 2.2 Eavesdropping range classification. (From Ranasinghe, D.C. and Cole, P.H., Confronting security and privacy threats in modern RFID systems. In *Proceedings of ACSSC 06*, 2006, pp. 2058–2064. With permission.)

Malicious scanning range: An adversary may build his own reader-archiving longer read ranges, especially if regulations about radio devices are not respected. A conversation between a reader and a tag can be eavesdropped over a greater distance than is possible with direct communication. For example, tags compliant to ISO 14443 have a reading distance of around 10 cm (using standard equipment). However, Kfir et al. showed that this distance can be increased to 55 cm employing a loop antenna and signal processing [36].

Eavesdropping is particular problematic for two reasons:

1. Feasibility: it can be accomplished from long distances.
2. Detection difficulty: it is purely passive and does not imply power signal emission.

Eavesdropping attacks are a serious threat mainly when sensitive information is transmitted on the channel. To give an example, we consider the use of RFID technology in payments cards (RFID credit cards) [37]. In an eavesdropping attack, information exchanged between the credit card reader and the RFID credit card is captured. Heydt-Banjamin et al. showed how this attack can be carried out [38]. An antenna was located next to an off-the-shelf RFID credit card reader. The radio signal picked up by the antenna was processed to translate it into human readable form. In particular, the following pieces of data were captured: cardholder name, complete credit card number, credit card expiry date, credit card type, and finally information about software version and supported communications protocols. As the above example shows, eavesdropping attacks should therefore be considered and treated seriously.

2.3.3 Authentication

Entity authentication allows the verification of the identity of one entity by another. The authenticity of the claimed entity can only be ascertained for the instant of the authentication exchange. A secure means of communication should be used to provide authenticity of the subsequent data exchanged. To prevent replay attacks, a time-variant parameter, such as a time stamp, a sequence number, or a challenge may be used. The messages exchanged between entities are called tokens. At least one token

has to be exchanged for unilateral authentication and at least two tokens for mutual authentication. An additional token may be needed if a challenge has to be sent to initiate the protocol.

In RFID context, the first proposals found in literature are based on unilateral authentication [39–41]. However, the necessity of mutual authentication has been confirmed in many publications [42–45]. In ISO/IEC 9784, the different mechanisms for entity authentication are described [46]:

- Part 1: General model
- Part 2: Entity authentication using symmetric techniques
- Part 3: Entity authentication using a public key algorithm
- Part 4: Entity authentication using a cryptographic check function

Use of a cryptographic check function seems to be the most precise solution for RFID. Due to the fact that standard cryptographic primitives exceed the capabilities of a great number of tags, the design of lightweight primitives is imperative, at least for low-cost RFID tags.

The two entities (claimant/verifier) share a secret authentication key. An entity corroborates its identity by demonstrating knowledge of the shared key. This is accomplished by using a secret key with a cryptographic check function applied to specific data to obtain a cryptographic check value. This value can be recalculated by the verifier and compared with the received value. The following mechanisms, as shown in Figure 2.3, are possible.

2.3.4 Skimming

Takashimaya, one of the largest retailers in Japan, now sells antiskimming cards called "Sherry" at their department stores. Consumers can just put the cards in their wallets to prevent their RFID-chipped train passes, etc. from skimming attacks.

The antiskimming card functions by creating a reverse electromagnetic field like Taiyo's technology [47].

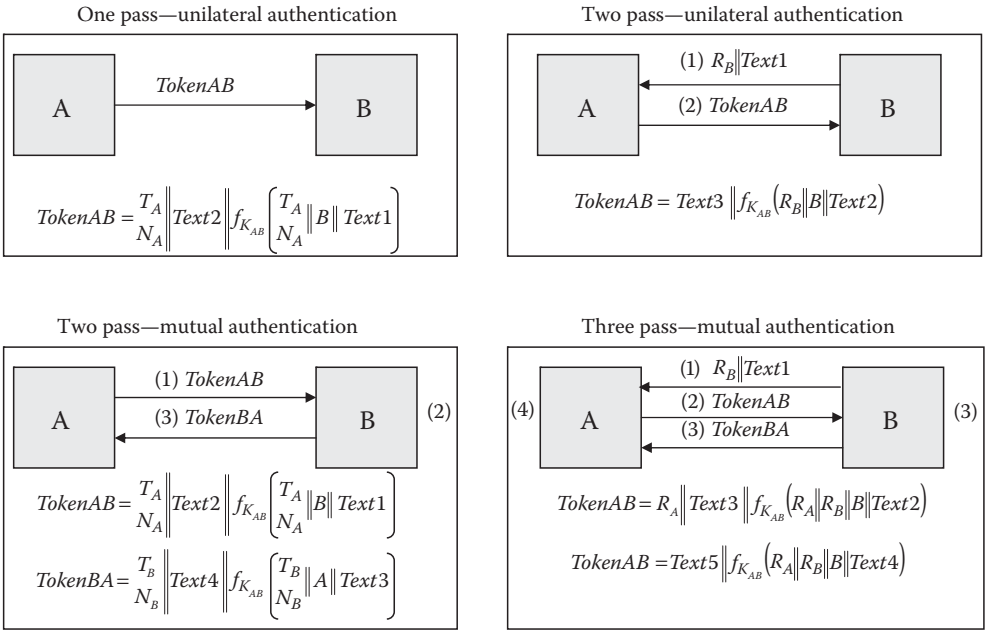


FIGURE 2.3 Entity authentication mechanisms.

Eavesdropping is the opportunistic interception of information exchanged between a legitimate tag and legitimate reader. However, skimming occurs when the data stored on the RFID tag is read without the owner's knowledge or consent. An unauthorized reader interacts with the tag to obtain the data. This attack can be carried out because most of the tags broadcast their memory content without requiring authentication.

One interesting project is the Adam Laurie's RFIDIOt project [48]. Specifically, RFIDIOt is an open source library for exploring RFID devices. Several experiments with readers operating at 13.56 MHz and 125/134.2 kHz are shown. The number of standards supported by the library is around 50. Some examples of the attacks carried out are the following:

Nonauthentication example: In 2004, Verichip received approval to develop a human-implant RFID microchip [49]. About twice the length of a grain of rice, the device is typically implanted above the triceps of an individual's right arm. Once scanned at the proper frequency, the Verichip answers with a unique 16 digit number which can correlate the user to the information stored on a database. The type of tag used by Verichip appears to be an EM4x05. This kind of tag can be read simply with the program "readlfx.py," obtaining the following information: card ID, tag type, application identifier, country code, and national ID.

Password authentication example: Since 2003, the Oyster card has been used on Transport for London and National Rail services. The Oyster card is a contactless smart card, with a claimed proximity range of about 8 cm, and based on Philips's MIFARE® standard [50]. A code for attacking this kind of card is included. The sample program "bruteforce.py" can be run against it, and it will try to log in the sector 0 by choosing random numbers as the key.

Nowadays, the security of e-passports have aroused a great interest [16,17,51,52]. Skimming is problematic because e-passports possess sensitive data. The mandatory passive authentication mechanism demands the use of digital signatures. A reader will be able to verify that the data came from the correct passport-issuing authority. However, digital signatures do not link data to a specific passport. Additionally, if only passive authentication is supported, an attacker equipped with a reader could obtain sensitive information such as your name, birthday, or even your facial photograph. This is possible because readers are not authenticated—in other words, the tag answers indiscriminately. Certain projects exist which give the code needed to read e-passports: RFIDIOt (Adam Laurie) [48], OpenMRTD (Harald Welte) [53], and JMRTD (SoS group, ICIS, Radbound University) [54].

2.3.5 Cloning and Physical Attacks

Symmetric-key cryptography can be used to avoid tag cloning attacks. Specifically, a challenge–response like the following can be employed. First, the tag is singulated from many by means of a collision-avoidance protocol like the binary tree walking protocol. The tag (T_i) shares the key (K_i) with the reader. Afterward, the following messages are exchanged:

1. The reader generates a fresh random number (R) and transmits it to the tag.
2. The tag computes $H = g(K_i,\ R)$ and sends back to the reader.
3. The reader computes $H' = g(K_i',\ R)$ and checks its equality with H.

The g function can be implemented by a hash function or, alternatively, by an encryption function. Note that if the g function is well constructed and appropriately deployed, it is infeasible for an attacker to simulate the tag. Because standard cryptographic primitives (hash functions, message authentication codes, block/stream ciphers, etc.) are extravagant solutions for low-cost RFID tags on account of their demand for circuit size, power consumption, and memory size [55], the design of new lightweight primitives is pressing.

For some kinds of tags, resources are not so restricted. However, their cost is much higher than low-cost RFID tags (i.e., tags used in supply chain). An example of these sort of tags are e-passports. The active authentication method is an anticloning feature. The mechanism relies on public cryptography. It works by having e-passports prove possession of a private key:

1. The tag generates an 8 bytes nonce and sends it to the tag.
2. The tag digitally signs this value using its private key and transmits it to the reader.
3. The reader can verify the correctness of the response with the public key supposedly associated with the passport.

Tamper-resistant microprocessors are used to store and process private and sensitive information, such as private keys or electronic money. The attacker should not be able to retrieve or modify this information. To achieve this objective, chips are designed so that the information is not accessible using external means and can only be accessed by the embedded software, which should contain the appropriate security measures.

Making simple electronic devices secure against tampering is very difficult, as a great number of attacks are possible, including [56]:

- Mechanical machining
- Laser machining
- Energy attacks
- Temperature imprinting
- Probe attacks
- Active or injector probes
- Energy probes
- Manual material removal
- Clock glitching
- Electronic beam read/write
- Imaging technology
- Water machining
- Shaped charge technology
- Radiation imprinting
- High-voltage imprinting
- Passive probes
- Pico probes
- Matching methods
- High or low voltage
- Circuit disruption
- IR laser read/write

  ⋮

As sensitive information such as cryptographic keys are stored on the chips, tamper-resistant devices may be designed to erase this information when penetration of their security encapsulation or out-of-specification environmental parameters is detected. Some devices are even able to erase all their information after their power supply has been interrupted.

In the RFID context, we have to distinguish between low-cost RFID tags and tags used in applications without severe price restrictions. Low-cost RFID tags are very constrained resources (storing, computing, and energy consumption). These kinds of tags are usually nonresistant to physical attacks. An example of these kinds of tags are tags compliant with the EPC Class-1 Generation-2 specification [57]. High-cost tags, sometimes called contactless chips or smart cards, are not so restrictive