

Copyright © 2007 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

S. C. G. Periaswamy, S. Bharath, M. Chagarlamudi, S. Estes, D. R. Thompson, "Attack graphs for EPCglobal RFID," in *Proc. IEEE Region 5 Technical Conf.*, Fayetteville, Arkansas, April 20-21, 2007, pp. 391-396.

# Attack Graphs for EPCglobal RFID

Senthilkumar Chinnappa gounder Periaswamy, Suman Bharath, Manideep Chagarlamudi, Scott Estes, Dale R. Thompson

Computer Science and Computer Engineering Dept., University of Arkansas  
E-mail: {schinna, sbharath, mchagar, sketes, drt}@uark.edu

**Abstract-RFID uses radio frequency signals to provide a no-contact and non-line-of-sight identification. In spite of its numerous advantages and implementations, it can also pose invasive new threats to rights, privacy of individuals, and security of organizations. A modified version of attack graph, a graph-based approach to network vulnerability analysis, is used in the threat modeling of an EPCglobal RFID system. The model can be used for the qualitative and quantitative assessment of the vulnerabilities and security attributes of the system.**

## I. INTRODUCTION

### A. Problem

Radio frequency identification (RFID) uses radio signals to automatically identify objects like a barcode is used to identify objects in a retail store [1]. It is used in many different applications such as gas payment, toll roads, automobile anti-theft systems, pet identification, entry cards, humans, and the supply chain. The most common form of RFID is the Electronic Product Code (EPC) system managed by EPCglobal Inc. [2]. EPC is a technology similar to the uniform product code (UPC) barcode identification except that it uses wireless signals instead of optics.

RFID can provide huge benefits to society. But it can also pose invasive new threats to rights, privacy of individuals, and security of organizations [1].

- What if an attacker performs an unauthorized inventory of a store by scanning RFID tags with a reader or deletes the serial number on RFID tags in the store disrupting business operation?
- What if an attacker plants a smart bomb that explodes when there are five or more Americans with RFID-enabled passports detected in a restaurant?

To receive the benefits of RFID tags, we must define and overcome security problems such as the violation of user privacy. An unbiased threat model of RFID needs to be performed to determine the threats to RFID and the threats by RFID to the privacy of individuals.

Once the threats are identified, a proper method is needed for the qualitative and quantitative assessment of vulnerabilities and security attributes of the system [6]. The developers and users of the system should be able to prioritize their security

measures based on the risk assignment of the components of the system. A reliable tool should be developed to test the effectiveness of these changes and new implementations.

## II. LITERATURE REVIEW

RFID is the latest phase in the decade-old trend of the miniaturization of computers [4]. RFID stands for radio frequency identification and describes the use of radio frequency signals to provide automatic identification [5]. RFID technology is no-contact and non-line-of-sight identification, which is different from ubiquitous barcode identification technology [6]. The electronic product code (EPC) was developed by the Auto-ID Center at MIT and is now being managed by EPCglobal Inc. EPCglobal Inc. is a global not-for-profit standards organization commercializing the Electronic Product Code™ (EPC) and RFID worldwide [1].

RFID systems consist of radio frequency (RF) tags and RF tag readers. The reader interrogates the tag for its content by broadcasting an RF signal. The tag responds by transmitting back resident data, typically including a unique serial number [7]. The unique serial number interacts with the in-house database to do the necessary operation. The potential features of RFID have enabled its deployment in a wide range of applications including supply chain management, manufacturing, retailing, auto payment systems, animal identification, smart cards and health care. While expectations for RFID are growing, more concerns are being raised about its use [8]. RFID can pose new invasive threats to rights, privacy of individuals and security of organizations [9], [1]. The threat to the privacy of an individual and security of the RFID system is being analyzed in [10]. Data from RFID tags can be modified to exploit back-end software systems using a SQL injection or buffer overflow [11].

Threats are potential events that cause a system to respond in a way in which it was not designed, including a damaging way. Threat modeling is a formal security analysis of a system to determine the highest risks and to identify how attacks occur [12]. It helps designers understand the view of an attacker, the security of the system, and the threats. The goal of threat modeling is to determine which threats are most serious and to identify techniques that mitigate them.

The steps to threat modeling include assembling a team, decomposing the system into threat targets, identifying threats to the threat targets, building one or more threat trees sometimes called attack graphs for each threat target, assigning risk to each threat, sorting the threats from highest to lowest risks, and proposing and evaluating techniques to mitigate the threats with higher risks [12], [13].

Initial work on categorizing threats can be found in [1]. The model STRIDE was applied to RFID to categorize threats [1]. STRIDE is an existing formal security-based analysis that categorizes threats [12]. Examples of STRIDE threats from [1] include:

- Spoofing identity: A competitor or thief performs an unauthorized inventory of a store by scanning tags with an unauthorized reader to determine the types and quantities of items.
- Tampering with data: A terrorist or criminal modifies a passport tag to appear to be a citizen in good standing.
- Repudiation: A retailer denies receiving a certain pallet, case, or item.
- Information disclosure: A competitor or thief performs an unauthorized inventory of a store by scanning tags with a reader to determine the types and quantities of items.
- Denial-of-service: An attacker kills tags in the supply chain, warehouse, or store disrupting business operations and causing a loss of revenue.
- Elevation of privilege: A user logging on to the database to determine product information can become an attacker by raising his/her status in the information system from a normal user to an administrator and write or add malicious data into the system.

An attack graph is a graph-based approach to network-vulnerability analysis. It can identify the set of attack paths through which an intruder or attacker achieves the target [14]. Each node in the attack graph represents a possible attack state. System state includes level of penetration by the attacker and configuration/state changes achieved on specific physical machine(s). Edges represent a change of state caused by a single action taken by the attacker and are weighted by some metric (such as attacker effort or time to succeed). Templates list the required condition for state transition. A major innovation of attack graphs over other vulnerability analysis methods is that it considers the physical network topology in conjunction with the set of attacks in a dynamic fashion [6].

The generation of attack graph is based on three inputs: attack templates, a configuration file and an attacker profile [14]. Attack templates represent a database of generic attack steps including necessary and acquired state attributes. The known and common attacks are broken into all possible atomic steps. The configuration file contains initial architectural information about the specific system. It also includes categorical labels for all known exploitable configurations that are used as

triggers for state changes. The attackers profile contains categorical information about the assumed capabilities of an attacker like the computing facilities he might possess and his physical access to the system. This is decided based on the security-level of the system and the type of attacks that are expected on the system.

The building of the attack graph can be initialized from either the goal/target state or start/initial state. The current state is matched with the states in the attack templates. The corresponding states on matching with the configuration and capabilities are customized to form the attack graphs. This process is repeated till the desired state is reached. Though attack templates represent pieces of known attack paths or hypothesized methods of moving from one state to another, their combination can lead to description of new attack paths [6].

Each edge has a weight representing a success probability, average time to succeed, or a cost/effort level of an attacker. This weight is a function of configuration and attackers profile. Several ways to estimate edge weight are given in [14]. A shortest path in the attack graph represents a low-cost attack. A set of near optimal paths based on the probability assigned to the edges is selected using an algorithm like shortest path algorithm. These paths indicate the most exploitable components of the system configuration.

Initially, red teams created attack graphs manually [12], [13], which are prone to error and is difficult for larger systems. An attack-centric approach for automatically generating attack graphs was proposed in [14], [6] and a more compact representation in [15]. A more general approach leverages symbolic model checking algorithms to automatically create attack graphs [16], [17]. In [18], adjacency matrix clustering is applied to attack graphs to correlate, predict, and hypothesize the attack steps in a system. A forward-search, breadth-first and depth limited algorithm to generate the attack steps and the tool to generate the attack graph is implemented in [19].

### III. OBJECTIVE

The objective of this research is to identify and categorize the threats to the security of the EPCglobal RFID system and the threats to privacy by it, decompose these threats to the threat targets, and build attack graph for threat targets.

### IV. METHOD

The authors reviewed the literature, created a list of threats, generated configuration files, hypothesized the attackers' capabilities, and created attack templates. Then, the attack graph was created using the threat target as the initial node. Finally, the attack graphs were used to analyze attacks. The EPCglobal Class-1 Generation-2 UHF RFID protocol [20] was considered as the specification for the RFID system.

### A. Threats

A list of threats to the system and by the system was identified and studied from the threats given in [1]. The threats included the security and privacy issues based on known attacks and attack that are possible on the system.

To generate of attack graphs for these threats, these threats were decomposed into threat targets. These threats targets are the states which an attacker or intruder tries to achieve in the system. These threat targets were categorized based on social and economical conditions so that the team could select the top priority threats for the generation of attack graphs. The team identified unauthorized modification of data in a tag and the unauthorized killing of a tag as likely threats.

### B. Inputs for the attack graph

The configuration file, attackers capabilities, attack templates of an EPCglobal RFID system were generated as inputs for the generation of attack graphs.

The configuration file is based on the EPCglobal Class-1 Generation-2 UHF RFID protocol specification [20]. The enhanced security features of the Class-1 Generation-2 were taken in consideration during the generation of the configuration files.

The attackers profile was created based on the assumed capabilities of an advanced level of attacker who is equipped with expensive measuring equipment. He may have access to the best possible facilities and can attain maximum privileges in the system using the computing resources available to him.

A subset of attack templates for the EPCglobal RFID system was generated from known possible and assumed attacks on the system.

### C. Generation of attack graphs

The threat target was made as the initial node of the attack graph. Each node contained the vulnerabilities of the system in the current state, the assumed capabilities of the attacker and the current state of the system.

The goal node was matched with the nodes in the attack templates and a subset of matching attack templates was identified for further processing. Each template was checked with the current vulnerabilities and capabilities. If they matched, their customized version joined with the goal node through an edge.

The edge that connected the two nodes contained the action by the attacker or the intruder, which made the transition. The edge also contained the condition necessary for the action to

be completed. The action is written above the edges and the conditions are written below the edge. If there were multiple ways to make the transitions, they were denoted by multiple edges between the nodes.

The process of matching was recursively done on the new nodes formed until the initial or default configuration of the system was reached. If there was no match for any of the node, they were discarded assuming that these paths were not possible.

In this process, there were instances of duplicate nodes and redundant edges. Two common cases occurred and are shown in Fig. 1 and 2. The duplicate nodes were removed by merging the nodes and edges from all the nodes to a single merged node. Redundant edges were removed by creating multiple edges between the nodes.

Other threat targets were subsets of the other attack graphs. Therefore, to avoid redundancy and due to space constraints we replaced the whole subset by the threat target as shown in Fig. 3.

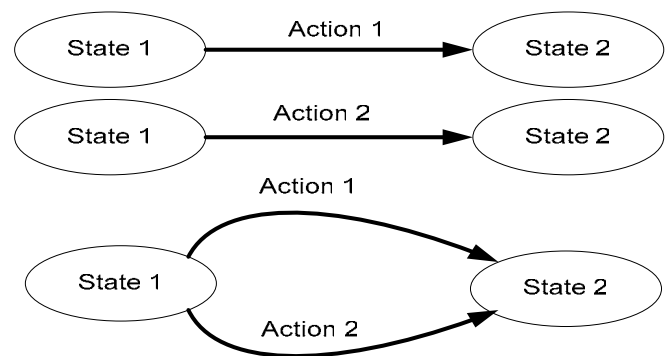


Fig. 1. Duplicate nodes.

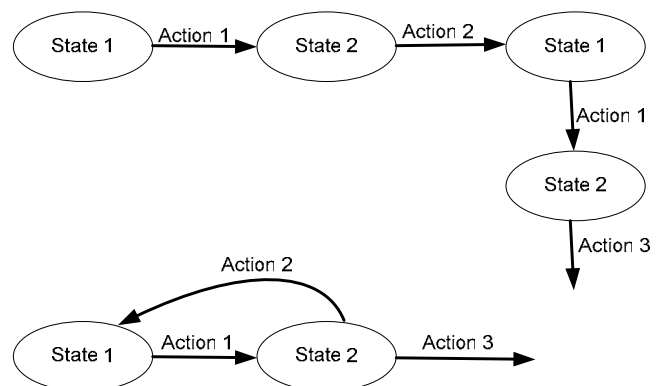


Fig. 2. Redundant edges

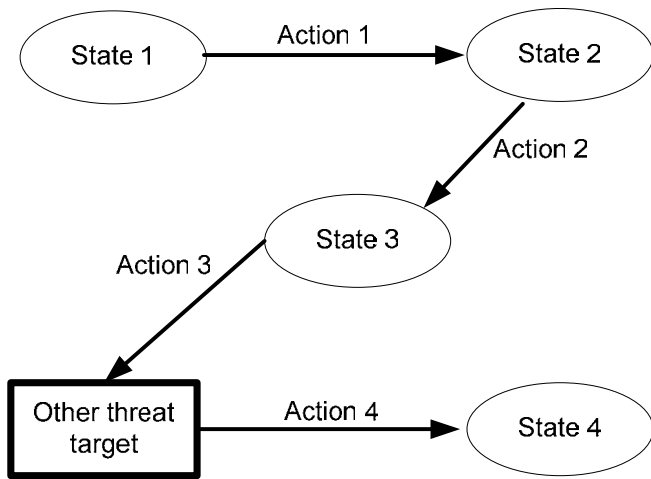


Fig. 3. Subset representing other targets

Using all the above methods, the two attack graphs modeling unauthorized modification of data in a tag and the unauthorized killing of a tag were the manually drawn.

*D. Analysis of attack graph*

A subset of the attack graph shown in Fig. 4 is considered for the discussion of how an attack is modeled. Due to space limitation, we were not able to present the complete attack graph in this paper.

Fig. 4 is a subset of an attack graph that shows how the data in a tag can be made inaccessible to the reader. The vulnerability of the system that is exploited is the reader's restriction of

communicating to only one tag at a time. The capability needed for an attacker is a blocker tag, which exploits the anti-collision protocols effectively performing a denial-of-service attack (spamming) on the reader [21]. This vulnerability of the system and capability required for the user is shown in the first node of Fig. 4.

The action that takes the system to a new state is the introduction of the blocker tag along with the other tags. This action is shown at the top of the first edge, which comes from the first node. The condition necessary for this action to be executed is physical access to the location of tags. This condition is shown below the first edge. The new state that results due to this action is the blocker tag repeatedly spamming the reader. This new state is shown in the second node of Fig. 4.

The attack is complete when the reader attempts to read tags in the presence of a blocker tag. This action is shown at the top of second edge of Fig. 4. The attack can continue if the reader does not have the capability to detect the presence of a blocker tag. This condition is shown at the bottom of the second edge. The final target state is shown in the third node of Fig. 4.

Assuming all edges have equal probability, physically damaging a tag and introducing a blocker tag are the easier methods for an attacker to kill a tag or make the tag data inaccessible to the reader. The subset of attack graph modeling physical damage to a tag is shown at Fig. 5.

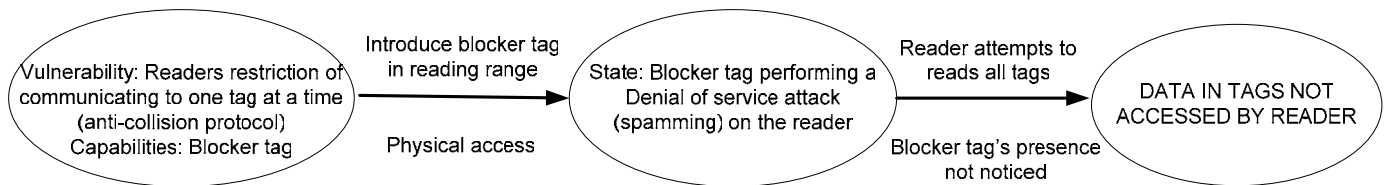


Fig. 4. Subset of an attack graph modeling blocker tag

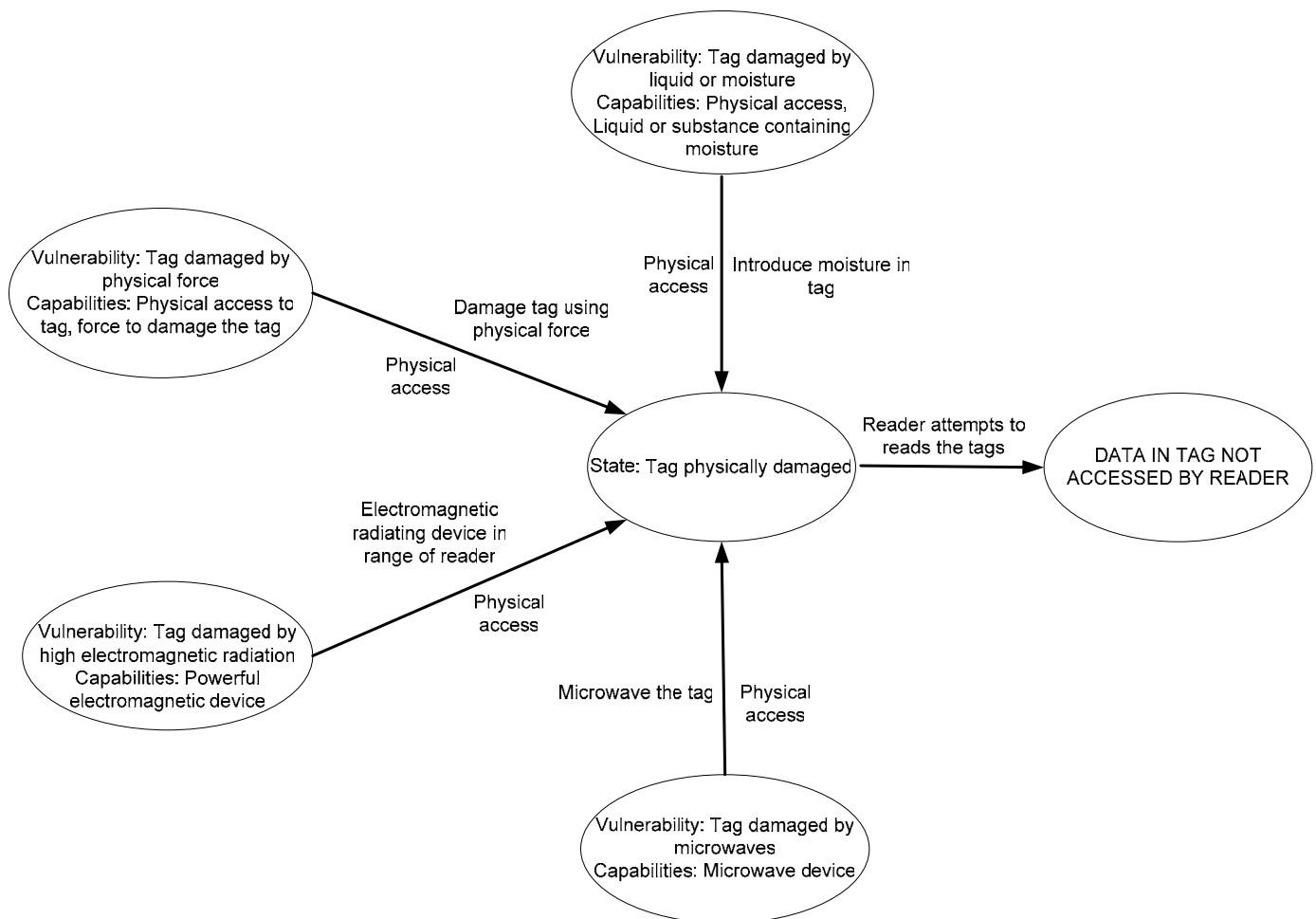


Fig. 5. Subset of an attack graph modeling physical damage to a tag

## V. FUTURE WORK

Attack graphs can be generated based on the vulnerabilities associated with the system, which could identify new threats to the system. This paper does not propose any formal methods for the calculation of probability in the edge due to absence of experimental data of these attacks. A method and data from experiments is needed for associating a probabilistic measure with the edges of the attack graph. Attack graphs can be generated for multiple attacker abilities with multiple probabilities associated with each edge. The implementation of various automated methods for generation of attack graphs should be done which will make the generation more scalable, reliable and accurate for large complex system. A simulation of the attacks on the system can be done based on the attack graphs.

## REFERENCES

- [1] N. Chaudhry, D. R. Thompson, and C. Thompson, *RFID Technical Tutorial and Threat Modeling*, ver. 1.0, tech. report, Dept. of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, Arkansas, Dec. 8, 2005. Available: <http://csce.uark.edu/~drt/rfid>
- [2] EPCglobal Inc., <http://www.epcglobalinc.org/>
- [3] L. P. Swiler, C. Phillips, D. Ellis, and S. Chakerian, "Computer-attack graph generation tool," in *Proc. DARPA Information Survivability Conf. & Exposition II (DISCEX)*, vol. 2, Jun.12-14, 2001, pp. 307-321.
- [4] RFID Viruses and Worms <http://www.rfidvirus.org/>
- [5] Intermec Technologies Corporation, "RFID overview." Available at: [http://epsfiles.Intermec.com/eps\\_files/eps\\_wp/IntroRFID\\_wp\\_web.pdf](http://epsfiles.Intermec.com/eps_files/eps_wp/IntroRFID_wp_web.pdf).
- [6] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID systems and security and privacy implications," in *Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, August 2002, pp. 454-470.
- [7] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems" in *International Conference on Security in Pervasive Computing*, Boppard, Germany, March, 2003, pp 454-469
- [8] CASPIAN, <http://www.nocards.org/>
- [9] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device" in *Proc. USENIX Security Symposium*, July-August 2005.
- [10] A. Juels, "RFID security and privacy: a research survey" in *IEEE Journal on Selected Areas in Communications*, Feb 2006, pp. 66-70.
- [11] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?" in *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, 13-17 March 2006, pp. 169-179
- [12] M. Howard and D. LeBlanc, *Writing Secure Code 2nd ed.*, Redmond, Washington: Microsoft Press, 2003.
- [13] P. Torr, "Demystifying the threat-modeling process," *IEEE Security & Privacy*, Sep. /Oct., 2005, pp. 66-70.
- [14] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proc. Workshop on New Security Paradigms*, Charlottesville, VA, USA, 1998, pp. 71-79.

- [15] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," in *Proc. ACM Conf. Computer and Communications Security (CCS)*, Washington, DC, Nov. 2002, pp. 217-224.
- [16] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *Proc. IEEE Symposium on Security and Privacy*, 2002, pp. 273-284.
- [17] S. Jha, O. Sheyner, and J. Wing, "Two formal analyses of attack graphs," in *Proc. Computer Security Foundations Workshop (CSFW)*, Jun. 24-26, 2002, pp. 49-63.
- [18] S. Noel and S. Jajodia, "Understanding complex network attack graphs through clustered adjacency matrices," in *Proc. Computer Security Applications Conf. (ACSAC)*, Dec. 5-9, 2005, pp. 160-169.
- [19] T. Zhang, M.-Z. Hu, D. Li and L. Sun, "An effective method to generate attack graphs," in *Proc. International Conference on Machine Learning and Cybernetics*, 2005, pp. 3926 – 3931.
- [20] *EPC™ Radio-Frequency Identity Protocols Class-1, Generation-2 UHF RFID protocol for communication at 860 MHz – 960 MHz*, ver. 1.0.9, EPCglobal Inc., Jan. 31, 2005. Available: <http://www.epcglobalinc.org/>.
- [21] A. Juels, R. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," in *Proc. Conference on Computer and Communications Security – ACM CCS*, October 2003.