FACTA UNIVERSITATIS
Series: **Automatic Control and Robotics** Vol. 13, N^{o} 2, 2014, pp. 97 - 105

SECURITY ISSUES IN INTERNET OF THINGS (IOT) RELATED TO PASSIVE RFID TAGS*

UDC ((004.7.056.6+004.56):RFID)

Dijana R. Vukovic[1,2]

[1]Department of Computer Science, University of Banja Luka, Faculty of Electrical, Banja Luka, Bosnia and Herzegovina
[2]Department of Telematics, Norwegian University of Science and Technology, Faculty of Informatics, Mathematics and Electronics, Trondheim, Norway

Abstract. *According to the latest research of emerging technologies in the next few decades, an era of fully integrated Future Internet is coming. The Internet of Things (IoT) paradigm will be the one of the leading technologies in the transformation from nowadays Internet into the Future Internet. Many European projects related to IoT were announced this year, such as Horizon 2020. In definition, IoT includes smart objects, machine to machine (M2M) communication, radio frequency (RF) technologies, and a central hub of information. One of the major requirements for IoT is that objects must have a unique identity, which would make them practically addressable when exchanging information. To achieve that, RFID tags can be used. There are three types of RFID tags: active, semi-passive, and passive. Considering their basic characteristics, passive tags are the most suitable to use in IoT. Passive RFID tags can have certain security issues. In this paper, using the STRIDE threat model, potential issues of passive RFID tags are described and discussed, with the currently known guidelines for their elimination.*

Key words: *RFID, Internet of Things (IoT), STRIDE, passive RFID tag security, threat model, security issues*

Received October 2, 2014
Corresponding author: Dijana R. Vuković
Department of Telematics, Norwegian University of Science and Technology, Faculty of Informatics, Mathematics and Electronics, O.S. Bragstads plass 2a, N-7034 Trondheim, Norway,
E-mail: dijana.vukovic@etfbl.net
* **Acknowledgement**: Dijana Vukovic, as a PhD student in the field of information security, is supported by the COINS Research School of Computer and Information Security.

1. INTRODUCTION

RFID (*Radio Frequency IDentification*) technology is one step to fully automatic identification system. Nevertheless, it is not a new technology. First appearance of RFID goes in the period of World War II, but it was patented for the first time in 70ies. Mario Cardullo's device was the first true ancestor of modern RFID: a passive radio transponder with memory. The first patent to be associated with the abbreviation RFID was granted few years after to Charles Walton in the early 80ies. A lot of effort was invested in RFID technology research and development since then. As a growing-up technology in last decade, it is used in different kinds of tracking systems (animal, postal package, airline baggage), in the automated toll collection, libraries, supply chain management, or passports. Nowadays, it is been an important part of IoT systems.

The very first definition of IoT derives from a "Things oriented" perspective - the considered things were very simple items: RFID tags. With objects tagged with RFID and paired with an IoT application, different kind of consumers can improve their everyday well being or even save money. For example, a grocery list could be automatically generated by smart fridges considering the expiration date of products in it. This kind of list reduces waste of money as the consumer doesn't purchase unnecessary items which leads to an overabundance of items with nearing expiration dates. One interesting combination of IoT and RFID tags in practical development certainly is iFridge, an intelligent fridge for food management based on RFID technology [1]. iFridge is an intelligent system which collects information about food with RFID tags in the fridge and based on that information suggests to an user some recipes for making meals. Also, it can be used as an reminder of lack of particular kind of food.

There are three types of RFID tags: active, semi-passive, and passive. Passive RFID tags are the most suitable to be part of IoT "things", mostly from the perspective of tags cost. From user perspective, the IoT systems have to protect their privacy and to provide them high level of security. As an indicator of importance of security issues and their countermeasures in IoT systems, Open Web Application Security Project (OWASP) started Top 10 project related to Internet of Things [2]. According to this project, 10 major vulnerabilities related to IoT systems in 2014 are: insecure Web interface, insufficient authentication/authorization, insecure network services, lack of transport encryption, privacy concerns, insecure cloud interface, insecure mobile interface, insufficient security configurability, insecure software/firmware, and poor physical security. Some of these might be caused by RFID tags, such as: insufficient authentication/authorization or insufficient security configurability.

Unfortunately, passive RFID tags can still have certain security issues, if they are not used right way. Since there is prediction that in the next few decades IoT will play important role in ICT technology growth, it is important to prevent this security issues to happen. If we observe the technology roadmap of IoT given in Figure 1, it is more than evident that IoT will be in the top of research and development until 2020 and even longer. IoT will be used in ubiquitous positioning (locating people and everyday objects) and physical-world Web (teleoperation and telepresence). Both of these will manipulate with sensitive data, and will be potential points of attack to malicious users. Using passive RFID tags in that kind of systems might be harmful. To prevent this, a security threat model for RFID systems has to be defined, altogether with the potential countermeasures

for identified threats. Well-defined threat model can be helpful for further application of passive RFID tags in IoT.

In this paper, STRIDE model is used for definition of RFID system's threat model. STRIDE is classification scheme for characterizing known threats according to the kinds of exploit that are used (or motivation of the attacker).

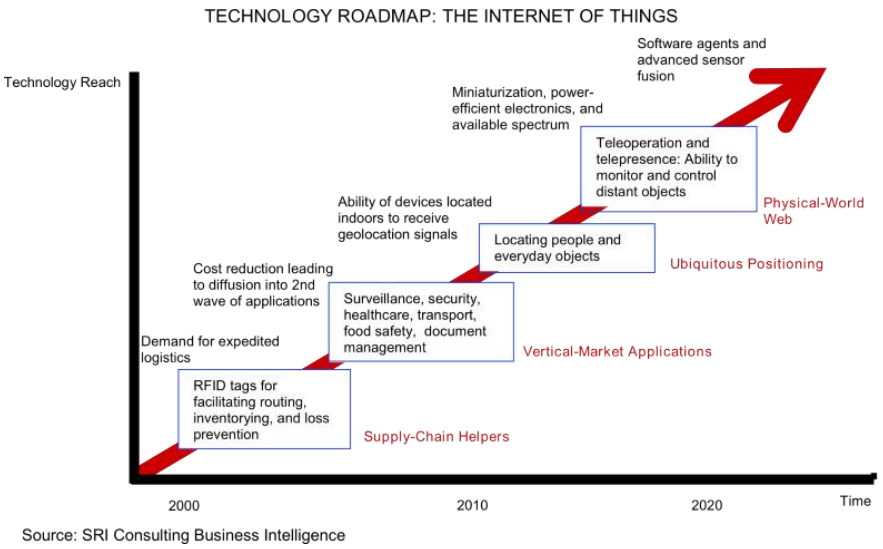

Fig. 1 Technology roadmap for IoT

The rest of the paper is organized as follows. In Section 2, basic terms of RFID systems and IoT are introduced and described. Section 3 gives an overview of IoT systems based on RFID tags. Security threats and countermeasures for the passive RFID using STRIDE threat model are given in Section 3. The paper is concluded in Section 4.

2. RFID AND INTERNET OF THINGS - TERMS AND CORRELATIONS

RFID technology is a major breakthrough in the embedded communication paradigm which enables design of microchips for wireless data communication. They help in the automatic identification of anything they are attached to acting as an electronic barcode. Three basic components of RFID systems are: RFID tag, RFID reader and back-end server (Figure 2).

RFID tag has a microchip that stores data and a coupling elements (a coiled antennas) to communicate via radio frequency communications. Tags are characterized by a unique identifier and can be applied to any kind of objects (even person or animal). They help in the automatic identification of anything they are attached to, acting as an

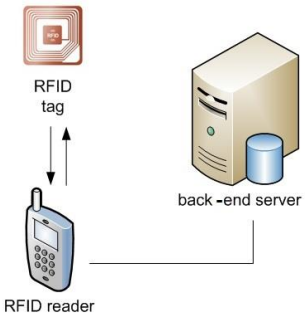

Fig. 2 RFID system

electronic barcode. RFID reader consists of a radio frequency module, a control unit, and a coupling element to interrogate the tags via radio frequency communication. RFID reader may contain internal storage, processing power, or an interface to back-end databases to provide additional function [3]. The back-end server in RFID systems is used for information storage, such as tag id, different type of reports, etc. RFID systems can be used to monitor objects in real-time, without the need of being in line-of-sight (mapping the real world into the virtual world). Therefore, they can be used in an incredibly wide range of application scenarios, spanning from logistics to e-health and security.

There are three types of RFID tags: passive, active, and semi-passive. Active tags have their own on-board power source and can initiate communication. Semi-passive tags also have an on-board battery, but they cannot initiate communication. They have long range, and often are very expensive. Passive tags are inactive until the reader "wakes" them up, they are cheap, and have short range. They have no ability to sense the channel, detect collisions, and communicate with each other. They respond only at reader commands.

From the frequency point of view, active RFID systems typically operate in the ultra-high frequency (UHF) band with frequency from 300 MHz to 3 GHz and offer a range of up to 100 m. Active tags are used on large objects, such as rail cars or big reusable containers. Passive RFID systems can operate in the low frequency (LF, covers frequencies from 30 KHz to 300 KHz), high frequency (HF, covers frequencies from 3 to 30 MHz) or ultra-high frequency (UHF) radio bands. As passive system ranges are limited by the power of the radio signal reflected from the tag back to the reader, they are typically less than 10 m. Passive RFID solutions are useful for many applications, such as: tracking of goods in the supply chain, authentication of products such as pharmaceuticals, and embedding RFID capability in a variety of devices.

Major disadvantage of passive RFID tags is their computational limitation for use of well-known and secure cryptoalgorithms. Consequence is lack of security comparing to other two type of RFID tags. Nevertheless, considering the fact that they are cheap, they are still used for different purposes (e.g. IoT systems).

Objects in IoT are sensed through RFID or sensors, achieving the integration of human society and the information system. Sensor networks also play a crucial role in the IoT. They can cooperate with RFID systems to better track the status of things (location, temperature, etc).

There are different definitions of IoT. **Internet of Things (IoT)** is a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. It can offer specific object identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These things are to be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability [4]. IoT is a new network that interconnect the wireless sensors and radio frequency identification (RFID) sensing devices through a wireless network and Internet technologies to achieve the overall perception of information, reliable transmission, and intelligent processing.

The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service. IoT can be considered as a new revolution of the Internet. In IoT, objects make themselves recognizable and they obtain intelligence by making or enabling context related decisions thanks to the fact that they can communicate information about themselves. They can

access information that has been aggregated by other things, or they can be components of complex services.

There are three basic IoT components [5]:

- Hardware – made up of sensors, actuators and embedded communication hardware,
- Middleware – on demand storage and computing tools for data analytics and
- Presentation – novel easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications.

3. The Internet of Things Based on RFID

IoT will offer specific object-identification sensors and connection capability as the basis for the development of independent federated services and applications, As it is explained in previous sections, RFID can be (is) used for an object-identification in IoT systems.

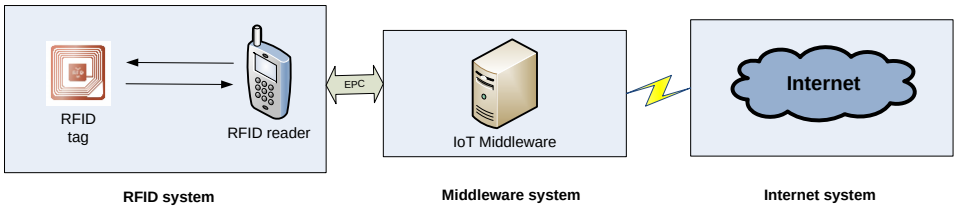

Fig. 3 IoT based on RFID

IoT system based on RFID usually consists of three parts: RFID system, middleware system and Internet system (Figure 3). In RFID system, RFID reader reads EPC (Electronic Product Code) from appropriate RFID tag and exchanges the code with middleware system over IoT middleware. Internet system usually consists of computer system and network server. EPC is unique identifier of each RFID tag. IoT middleware, according to [6] has to have following functionalities to manage interaction with a variety of devices: interface protocols (providing technical interoperability), device abstraction (providing an abstract format to facilitate the interaction of the application components with devices), central control, context detection and management (supporting context-aware computation), and application abstraction (provides an interface for both high-level applications and end-users to interact with devices). There are some open source middleware for IoT, such as OpenIoT [7]. OpenIoT is an open source middleware for getting information from sensor clouds, without worrying what exact sensors are used.

4. Security Threats and Countermeasures for Passive RFID Tags

Three main physical components of IoT are: RFID, WSN (*Wireless Sensor Network*) and the cloud, and all three of them can be vulnerable to particular type of attacks. WSN can be vulnerable on outside attacks (attacks from nodes which do not belong to a WSN),

interruption, interception, modification, host-based attacks, network-based attacks, etc [8]. Cloud can have huge set of vulnerabilities. The most common are: securely transferring data, accessing the data, data backup, password use, and privacy. Security is critical to any kind of network or software product and the first line of defense against data corruption is cryptography.

As one of the components, RFID tags (particularly passive) are mostly interesting to malicious attackers, since they allow person tracking as well as the objects and no high level intelligence can be enabled on these devices. However, these complex problems have solutions that can be provided using cryptographic or some other security protection methods and they have to be more researched before they are widely accepted. In that purpose, threat model can be very useful.

As the basic security goals, CIA triad (Confidentiality, Integrity, Availability) are recommended from different security organizations. **C**onfidentiality can be defined as an ability to hide information from those people unauthorized to see it. **I**ntegrity, on the other hand, is the ability to ensure that data is an accurate and unchanged of the original secure information. **A**vailability has to be provided because it is important to ensure that information concerned is readily accessible to authorized viewer all the times. Since IoT is identified as one of the technologies that will achieve growth in the next five years, people are concerned of the influence that IoT will have to their ordinary lives. In July 2014 Fortinet, a global leader in high-performance network security, published the results of an global survey titled "Internet of Things: Connected home" [9]. 57% of participants in survey were concerned about privacy and trust issues in IoT, and 67% were concerned about data privacy. Leak of confidentiality and integrity can lead to privacy and trust issues. Prediction from the same survey is that 61% homes will became "connected homes" until 2020. Accordingly, availability is also one important security goal that has to be fulfilled in IoT.

To fulfill security goals in general, it is important to have well-defined threat model that will be useful for identifying potential security threats and their countermeasures. In [10], as a threat model for RFID security, STRIDE [11] is suggested. STRIDE is classification scheme for characterizing known threats according to the kinds of exploit that are used (or motivation of the attacker)The model has six threat categories (Figure 4). An application of STRIDE model for identifying security threats of passive RFID tags is given as the following.

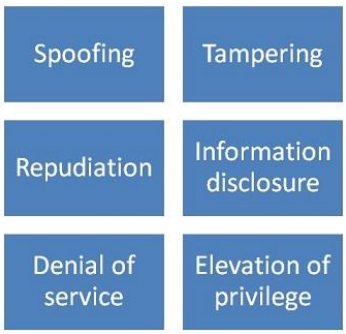

Fig. 4 STRIDE threat model

Spoofing. When an attacker comes into credentials possession of an authorized system user, spoofing might occur. To provide authentication mechanism for RFID tags, different RFID mutual authentication protocols were developed. Most of them were proved as inefficient. Passive RFID tags has limited memory and computational power and they use lightweight RFID mutual authentication protocols. Safkhani et. al. [12] described two protocols for passive RFID tags: one uses lightweight stream-cipher WG-7 to provide confidentiality and authenticity, and the other one uses one-way hash functions. Both of these protocols are proved as vulnerable to *tag impersonation attack* (a forgery attack in which the reader accepts a spoofed tag as a legitimate tag, and the modification for vulnerability removal is proposed. Any secure RFID authentication protocol must provide resistance against all kind of forgery attacks, include tag impersonation attack.

Tampering. Tampering in RFID systems occurs when attacker manipulates with data (modifies, adds, deletes, or just reorders data). The tampering has many dangerous effects, such as incoherence in the information system, exposure to opponent attacks, and mistakes in the production flow. There are two kinds of protections against tampering [13]: tamper-evidence (the feature of a process, device, or software, to detect the existence of tampering) and tamper-resistance (the ability to resist to tampering). Low cost RFID tags are very simple devices without a microprocessor, which implies the hardware tampering possibility is pretty high. Tampering actions may aim at damaging the device or at altering the system to access the code in order to reprogram it with a malicious one (e. g. code that will be able to execute insider attacks). In paper [14] fragile watermarking for RFID data tamper detection is proposed as a countermeasure for data tampering. The other possible solution is write activity record for RFID data tamper detection [15]. Watermarking is the art of embedding data directly within content, which is imperceptible to humans but readable by computers. In [16] a novel watermarking based tamper detection solution for low cost RFID passive tags which uses the 32 bit kill password as the cover medium is proposed. It can detect tampering anywhere in the RFID tag.

Repudiation. Repudiation occurs when a user denies an action and no proof exists to prove that the action was performed [10]. To prevent this, a non-repudiation protocol is required. The passive RFID tags has a limitation considering the memory and the computational power aspects. They are not suitable for a non-repudiation protocol, which usually requires existing of digital signatures, timestamps, or an audit trial. The back-end server has to enable non-repudiation protocol appliance in the data processing.

Information disclosures. Information disclosure occurs when information is exposed to an unauthorized user [10]. This can be threat to privacy, if the exposed information are individual (e.g. a fixed reader at a retail counter identifies the tags of a person and use that to provide individualized marketing [10]). One of the problems in low-cost passive RFID tags is that they do not provide authentication and privacy. As a solution for this issue, PAP [17] and IPAP [18] were proposed. PAP was proposed in 2009 and IPAP (as an improved PAP) was proposed one year after. PAP uses hash lock functions. Nevertheless, it might cause the privacy issues. IPAP has lower computation overhead. In PAP protocol, it is assumed that unauthorized reader (attacker) does not exist in the store. However, there is possibility of such case. This fact was used in IPAP, to solve the privacy issues from PAP. To prevent information disclosure without using of protocols, the killing tag, or the blocker tag can be used (non-cryptographic scheme).

Denial of service (DoS). Considering the fact that DoS denies service to valid users, DoS attacks can be easy accomplished and difficult to protect against. An attacker can shield the tag from being read with a Faraday Cage. In the debate over embedding tags in passports, it has been suggested that the passports have to be inserted into a foil holder to prevent this type of attack [10]. One of the ultra lightweight techniques used to prevent DoS on RFID systems is the Gossamer protocol [xxx]. Gossamer protocol comprises three stages: tag identification phase, mutual authentication phase, and updating phase, and it is inspired by SASI scheme. This protocol is proven to be vulnerable to DoS by de-synchronization in [19], where an improvement of it has been proposed.

Elevation of privilege. It occurs when an unprivileged user or attacker gains higher privileges in the system than what he is authorized [10]. Using gained privileges, malicious data can be written in database (for example, using SQL injection attack) or in file system on back-end server. The authorization mechanism must be built in the back-end server.

Using STRIDE model, potential threats to passive RFID tags are identified, discussed, and countermeasures for their prevention are given. Given countermeasures can improve correct usage of passive RFID tags in IoT systems and help with user's privacy and security protection. Computational power of passive RFID tags is big issue, and since the set of secure algorithms that will provide privacy protection, there can be a lot of research on this topic in the future.

5. CONCLUSION

Privacy includes the concealment of personal information as well as the ability to control what happens with this information. Privacy is the most important part to everyday users of any type of ICT applications. It does not differs in IoT systems and application neither. RFID tags are one of the basic elements in such systems. To detect and/or manage RFID threats conventional security management approaches can be used. It is evident that the set of potential security threats to passive RFID tags is huge, and that the most proposed and developed security mechanisms are proved as insecure. In this paper, using STRIDE threat model, an overview of passive RFID tag is given, and this can be used as a guideline for secure using of passive RFID tags. The security of passive RFID tags is very actual research topic with a lot of problems to be solved. As one potential plan for the further work development of repudiation prevention systems on back-end servers can be defined.

REFERENCES

[1] L. Xie, B. Sheng, Y. Yin, S. Lu, X. Lu, "iFridge: An intelligent fridge for food management based on RFID technology," in *Proceedings of* U*biComp'13*, Zurich, Switzerland, 2013. [Online]. Available: http://www.ubicomp.org/ubicomp2013/adjunct/adjunct/p291.pdf

[2] OWASP Foundation, "OWASP Internet of Things top ten project," 2014. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014 [Accessed on November 2014].

[3] D. Shih, C. Lin, B. Lin, "Privacy and sec aspects of RFID tags," 2004. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.304.9121&rep=rep1&type=pdf [Accessed on November 2014].

[4] X. Jia, Q. Feng, T Fan, Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," *in Proceedings of International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, pp. 1282–1285, 2012. [Online]. Available: http://dx.doi.org/10.1109/CECNet.2012.6201508

[5] J. Gubbia, R. Buyyab, S. Marusic, M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Journal of Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.future.2013.01.010

[6] S. Bandyopadhyay, M. Sengupta, S. Maiti, S. Dutta, "Role of middleware for Internet of Things: A study," International Journal of Computer Science & Engineering Survey (IJCSES), vol. 2, no. 3, pp. 94–105, 2011. [Online]. Available: http://www.oalib.com/paper/2635746#.VI_k3FlwqUk

[7] OpenIoT, "Open source cloud solution for the Internet of Things," 2014. [Online]. Available: http://openiot.eu/ [Accessed on November 2014].

[8] T. Kavitha, D. Sridharan, "Security vulnerabilities in wireless sensor networks: A survey," Journal of Information Assurance and Security, vol. 5, pp. 31–44, 2010. [Online]. Available: http://www.mirlabs.org/jias/secured/Volume5-Issue1/vol5-issue1.html

[9] Fortinet Reveals, "Internet of Things: Connected Home," Survey Results, 2014. [Online]. Available: http://www.fortinet.com/press_releases/2014/internet-of-things.html [Accessed on November 2014].

[10] D. R. Thompson, N. Chaudhry, C. W. Thompson, "RFID security threat model," in *Proceedings Acxiom Laboratory for Applied Research (ALAR) Conference*, 2006. [Online]. Available: http://www.csce.uark.edu/~drt/publications/rfid-threats-alar-060303.pdf

[11] F. Swiderski, W. Snyder, *Threat Modeling*, Microsoft Press, 2004.

[12] M. Safkhani, N. Bagheri, M. Naderi, Y. Luo, Q. Chai, "Tag impersonation attack on two RFID mutual authentication protocols," in *Proceedings of Availability, Reliability and Security (ARES) Conference*, Vienna, pp. 581–584, 2011. [Online]. Available: http://dx.doi.org/10.1109/ARES.2011.87

[13] F. Gandino, B. Montrucchio, M. Rebaudengo, *Tampering in RFID: A Survey on Risks and Defenses*, Mobile Network and Applications, Springer, 2009.

[14] V. Potdar, C. Wu, E. Chang, "Tamper detection for ubiquitous RFID-enabled supply chain," Computational intelligence and security, Lecture Notes in Computer Science, vol. 3802, pp. 273–278, 2005. [Online]. Available: http://dx.doi.org/ 0.1007/11596981_40

[15] A. Yamamoto, S. Suzuki, H. Hada, J. Mitsugi, F. Teraoka, O. Nakamura, "A tamper detection method for RFID tag data," in *Proceedings of IEEE International Conference on RFID*, Las Vegas, USA, pp. 51–57, 2008. [Online]. Available: http://dx.doi.org/10.1109/RFID.2008.4519365

[16] A. N. M. Noman, K. Curran, T. Lunney, "A watermarking based tamper detection solution for RFID tags," in *Proceedings of Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP) Conference*, Darmstadt, pp. 98–101, 2010. [Online]. Available: http://dx.doi.org/10.1109/IIHMSP.2010.32

[17] A. X. Liu, L. A. Bailey, "PAP: A privacy and authentication protocol for passive RFID tags," Journal of Computer Communications Archive, vol. 32, no. 7–10, pp. 1194–1199, 2009. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2009.03.006

[18] S.-H. Kim, H.-J. Lee, H.-W. Jung, B. K. Maeng, Y. Park, "IPAP: Improved privacy and authentication protocol for passive RFID tags," in *Proceedings of Network Infrastructure and Digital Content, IEEE International Conference*, Beijing, pp. 30–34, 2010. [Online]. Available: http://dx.doi.org/10.1109/ICNIDC.2010.5657894

[19] D. Tagra, M. Rahman, S. Sampalli, "Technique for preventing DoS attacks on RFID systems," in *Proceedings of Software, Telecommunications and Computer Networks (SoftCOM) Conference, Split*, pp. 6–10, 2010. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5623669

[20] P. Peris-Lopez, J. C. Hernandez-Castro, J. M.E. Tapiador, A. Ribagorda, "Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol," Lecture Notes in Computer Science, vol. 5379, pp 56–68, 2009. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-00306-6_5