Security Threats and Challenges for RFID and WSN Integration

Mouza Bani Shemaili, Chan Yeob Yeun, Khalid Mubarak, Mohamed Jamal Zemerly
Electrical and Computer Engineering Department,
Khalifa University of Science, Technology and Research, Sharjah, UAE
mouza@kustar.ac.ae cyeun@kustar.ac.ae mubarak@kustar.ac.ae jamal@kustar.ac.ae

Abstract

Radio Frequency Identification (RFID) and Wireless Sensor Network (WSN) are the combined technologies that will spread in the near future to enter all of our everyday activities. However, the security of these technologies is very much vulnerable. Adding some security measures to small computation powered devices that cannot handle the available security algorithms is considered a challenge. However, even low powered devices must be protected in ways that will present sufficient computational challenges to adversaries. This paper introduces suggested steps to build a secure protocol for the combined RFID and WSN technology application systems. Moreover, it demonstrates the possible attacks and threats on these combined technologies by analyzing their system environment and finally it discusses the possible threats that may occur.

1. Introduction

Smart Sensor Network technology is the new integration of both of the Radio Frequency Identification (RFID) technology and the Wireless Sensor Network (WSN) technology. In order to reach the concept of the ‘Internet of things’ that connects the physical and virtual world using the internet, the merging of the two technologies is needed. Both of the RFID and WSN technologies connect the physical objects and their information with the virtual world. These two technologies can add the smartness specification on the physical objects so that objects can identify and specify their condition to the virtual system (backend server). However, both of these two technologies have been developed separately and have been treated as unrelated research areas.

Though, after realizing that both technologies can work together new researchers try to combine both technologies and come up with the new smart sensor Network technology. However, both technologies face some security issues so combining both of them will need more security attention. This paper tries to address the security threats on such combination and gives a guide on how to build a secure RFID/WSN application.

The paper is organized as follows: the next section introduces the technologies that we need to discuss which are: RFID, WSN and the integration of the RFID and WSN technologies. Then the paper illustrates some of the application examples that are enhanced by the integration of both technologies. The related work is explained in section 4. Section 5 discusses the threats and the attacks on both of the RFID and the WSN technologies. Also, section 6 gives a scenario of smart chain tracking system. Finally section 7 concludes the paper.

2. Background Technologies

This section describes the two technologies that lead to the smart environment. Therefore the section is divided into three subsections the first and the second section introduce the two used technologies which are: RFID and WSN. The third subsection specifies the benefit of the Integration of RFID and WSN.

2.1. RFID Technology

Radio Frequency Identification (RFID) is a generic term that is used to describe the technology that uses radio waves to automatically identify an object or a subject wirelessly. AIM Global is the association for the Automatic Identification and Mobility industry. AIM Global grouped RFID technology under the category of automatic identification technologies such as bar code, magnetic strips, optical character recognition, voice recognition, touch memory, smart cards, biometrics, etc. [1].These technologies are used to help machines to identify objects or subjects. There are several methods to do that, but the most common one is to store a unique serial number on a microchip that is attached to the object or the subject.

The RFID system consists of three components: a tag, a reader and a server. Fig.1 shows the RFID system components. The RFID tag is a microchip which consists of an antenna and a chip. Therefore, we can call the object or the subject, attached to the RFID tag a tagged item.

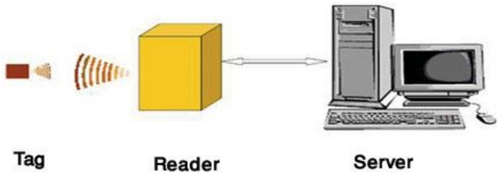

Figure 1. RFID System Components

There are three types of RFID tags: Passive, Semi-Passive and Active. Passive tags need to be beamed by the reader to be activated. Passive tags are also smaller, less expensive than the other kinds of tags and used for a short range [3cm – 3 m].

Semi passive tags have an on-board power source to run the tag chip circuit and draw the communication energy from the reader. Besides, semi passive tags have longer read range than passive tags.

Active tags include miniature batteries used to power the tag and to initiate the communication with the RFID reader. Active tags can be read from a distance of one hundred feet. Also, active tags can be used as sensors and are more expensive than the other kinds of tags. Active tags can be used indoor and outdoor. We also can classify tags depending on their internal memory type and size.

Smart tags have memories that can be written into and erased, while others are read-only tags that have memories that can only be read. Actually, the cost of a passive tag depends on the memory size that it contains.

The reader continuously emits radio signals in a given frequency. When a RFID tag enters the reader signals, it will be activated and the RFID tag antenna enables the chip to transmit the unique serial number wirelessly to the reader through the modulation of transmittance frequencies. Then, the reader converts the radio waves reflected back from the RFID tag into digital information that can then be relayed to the backend server for further processing of the acquired data [2]. For the RFID system to communicate, both of the RFID tag and the reader have to be tuned to the same frequency. RFID systems use many different frequencies [3], but generally the most common ones are as follows:

1. Low-frequency around 125-134 KHz
2. High-frequency 13.56 MHz
3. Ultra-high-frequency or UHF 860-960 MHz
4. Microwave 2.45 GHz and above is also used in some applications.

RFID technology can be used anywhere that needs a unique identification system and has been integrated in different area such as toll collection [4], agriculture [5], access control [6], supply chain [7], logistics [8], healthcare [9] and library [10].

2.2. WSN Technology

Wireless Sensor network (WSN) is a network that is capable of gathering sensory data from the deployed sensors in order to reply to a certain queries. The WSN consists of four main parts which are: the sensor field, sensor nodes, the sink and the base stations [11, 12]. Fig. 2 illustrates the WSN components.

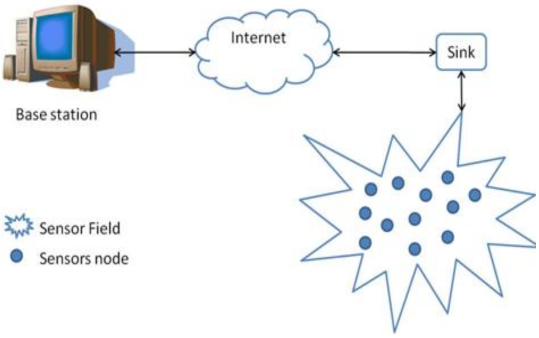

Figure 2. WSN components

The sensor field is the area in which the sensors nodes are placed to detect a particular phenomenon that is expect to occur. Sensors nodes or motes are tiny sensor nodes connected together through wireless links. They are in charge of collecting data from its surroundings (e.g. temperature, humidity, pressure) and routing this information back to a sink. Sensors communicate using multi-hop wireless connectivity because sensor energy cannot support long range communication to reach a sink. In order to forward data within the sensors network to a remote sink node router nodes are deployed. The sink sensor nodes are responsible of aggregating and storing the data from the other sensor nodes. The objective of the sink is to reduce the total number of messages that need to be sent.

The base stations are more powerful nodes that may operate as control nodes which extract information from the sensors network and send back the queries into the network. They can be considered as gateways to other networks and contain a powerful data processing/storage centre [13].

WSN technology uses three types of known protocols as its own standards which are: Wi-fi, Bluetooth, and Zigbee [14]. WSN integrates in different applications such as disaster prevention [15], healthcare [16], home automation [17] and intelligent transportation [18].

2.3. Integration between RFID and WSN

The integration of both of the RFID and WSN technology can deploy a smart object. RFID and WSN can complement each other by adding additional services for each. RFID technology is used to identify the location of the object while WSN is used to sense the object surrounding environment

[19, 20]. Thus, the combination of these two technologies will provide identity and location of an object along with information regarding the condition of the object that is attached to the sensors enabled RFID tag. Integration of the RFID and WSN can extend the read range so reader can read tags from 100-200m distance which is beyond the normal range of readers. This integration can add the multi-hop to the RFID application which can extend the capability of the application to operate in a wider area [21, 22, 23].

Researchers classify the RFID and WSN integration architecture based on the variety of applications. Authors in [24] classified the integration of integrated sensor-tags into two main classes based on the merging architecture in the pervasive computing environment. The first class is the integration of the sensors and tags with the RFID reader where the second class is the integration of the sensors and tags with the ad hoc network.

On the other hand, authors in [25] classified the integration of RFID and WSN into three classes which are: 1) Integration of Sensors into RFID Tags, 2) Integration of RFID into Wireless Sensor Networks, and 3) Integration of RFID System and Wireless Sensor Networks into a Network. The first class adds sensing ability to the RFID tags and the communication is done through the RFID reader. The second class is divided into two other subclasses which are: 1) Integration of the wireless sensor node with the RFID tags. The RFID tags in this subclass are able to communicate with the ad hoc network. 2) Integration of wireless sensor node with the RFID reader. The third class separate the RFID and WSN network physically so both technologies exist in the system yet, they work independently.

There are some several example applications that get the benefits from the integration of these two technologies. Next section introduces some of these applications.

3. Applications Example

Applications that need both of the RFID and WSN technologies are widespread in many aspects of real life areas. Some of these applications are:

3.1. Healthcare System

Healthcare system faced a lot of challenges that need to be solved such as geriatric monitoring, drug counterfeiting, medical errors, etc. All of these cases can be solved using RFID technology which has a potential in increasing the efficiency and utilization of the healthcare system. RFID technology can overcome previously mentioned challenges with low budget, high efficiency, and secure way.

RFID and WSN technologies can be used in many cases such as:

- Managing the location of the doctors, nurses, patient and medicine by tagging all of them with RFID tags.
- Finding the location of the doctors and the nurses in the system can determine the crowded areas and hours within the healthcare system. When the system have a bottleneck it is easy to find that area and improve the system there.
- Prevent drug counterfeiting.
- Inventory management for the out of the stack medicine
- Mange the old people at their home and report their movement to the hospital.
- Organizing the Doctor, nurse, and patient schedule.

However, there are some problems that may rise related to the use of a new technology in healthcare systems such as that it will take time to train and change the system infrastructure to adapt to the new technology [26, 27, 28].

3.2. Food Chain Tracking

This is defined as maintaining the food state (temperature and humidity) through the supply chain from the source to the destination. The food temperature and humidity can determine the quality and freshness of food when they are stored and shipped. RFID technology can be combined with wireless sensor network technology in order to gain a smart system during the life time of the food transmission from the source to the destination. Combining both technologies can provide a system that controls the food temperature, humidity, and visibility during the transmission. By inserting the RFID tag within each product container and placing WSN inside the shipment transportation the Cold chain logistic system can be tracked and managed. All of the tag and sensor data sent to the shipment transportation leader to make sure of the food statement. The shipment transportation leader relays this information back to the main system. This way the main source can track and manage its products during the transmission life time and provide the destination with information related to their shipment such as the location and the status of the delivered product [29], [30]. Till now there is no standard framework for the integration of the RFID and WSN technologies. In the next section some related work of the suggested and proposed RFID and WSN are discussed.

4. Related Work

Researchers are currently seeking feasible framework for the integration of the RFID and WSN. However, this is an emerging area and little has been done to find a framework that covers both of the technologies. One of the most suitable proposals is the Electronic Product Code (EPC) network framework.

The Auto-ID Center designed the EPC Network [31, 32] in order to links all the tagged objects in the world altogether through the internet. EPC network consists of four main parts as follow:

1. EPC

The EPC is a numbering standard that is considered as a globally unique identification object ID so that each item in the world can be assigned a unique identification number. The tagged object information is not stored using the EPC numbering standard. However, the EPC number is considered a reference to the tagged object's information that is stored on the backend database. The EPC numbering standard that varies from 64 to 256 bits long consists of four main parts which are Header, Manufacturer, Product and Serial Number. The header is used to define the number, type and the length of the consequent data partitions. The manufacture and the product portions are used to identify the individual item. The serial number is used to identify a unique object identifier. Fig.3 shows the EPC format.

MSB			LSB
Header	Manufacturer	Product	Serial Number

Figure 3. EPC Format

2. RFID Tag and Reader

RFID tags store the EPC in order to allow business partners to share information about their products and processes. Therefore, when an RFID tag communicates with an RFID reader it sends its EPC. Then, the reader delivers the EPC to the backend server used as tagged object information reference.

3.Object Name Service (ONS)

The Object Name Service function is similar to the Internet's Domain Name Service (DNS). It is a directory service that routes requests. ONS uses the EPC after resolving it and locates the directory of that EPC manufacturer and the offering information about the product on the EPC Network.

4. EPC Information Service (EPCIS)

The EPC Information Service (EPCIS) is considered as a gateway that enables EPC requester information to exchange EPC-related data. At the EPC Network the EPCIS works as a repository that stores the product information and allows any trading partners to offer their product information services. Therefore, EPCIS is considered as an interpreter between the database and the application user.

This way, the EPC network connects the physical world with the virtual world and facilities the process of tracking the tagged objects via the internet. Now there are some research areas that impose the idea of the EPC network as a foundation framework for both of the RFID and WSN technologies such as Sung et al. [33] who proposed the EPCglobal standard architecture as a base for the integration of the RFID and WSN technologies. The basic aim of the EPC sensor network is to collect the data from tagged objects and sensors. Tagged data and sensors read by the RFID reader which relays data to the Application Level Event middleware (ALE). ALE reduces the data volume by filtering and grouping the data depending on the client request. Then, the ALE reports to the end user with the useful information. Also, the system adopts the two services which are: the Object Naming Service (ONS) and EPCIS service. ONS returns the IP address of the server depending on certain information related to EPC. Whereas, EPCIS service is considered as a repository of the sensing and the RFID data. The EPCIS information can be accessed by the client in order to use its stored data in different application services depending on its need.

Wang et al. [34] adapt the idea of the EPC Sensor Network (ESN) architecture as a basis of the integration technologies of RFID and WSN. Also, the paper proposed the use of the Complex Event Processing (CEP) to build a middleware system to filter the two types of data which are RFID and Sensor data. Then, the middleware groups and aggregates events data in real time. Finally, it provides data report to the upper layer.

However, none of the research direction that we read so far tries to discuss the building of the EPC Network for the integration of both of the RFID and WSN technologies in a secure way. This paper provides the first step of building an integrated system of both of the RFID and WSN in a secure way by analyzing the surrounding area and identifying the threats and attacks on the system as explained in the next section.

5. Security Challenges and Attacks

As wireless networks become ubiquitous and their security becomes important, hackers have found it relatively easy to break into. RFID and WSN technologies are considered wireless communication systems. The problem lies with the difficulties in tracking attacks in the open RF environment. Consequently, there are great demands to improve the security of the RF system.

The main issues with most of today's systems or applications that they are built without any security aspect. Therefore, system designers must integrate the security of all the system components. Since components designed without any security aspect can become a point of attack to that system. Limited memory and power limitation devices such as sensor nodes and RFID tags are very much vulnerable as they face some major security challenges and threats.

Therefore, any proposed system architecture must be built with security aspect in mind. The system must provide the general security aspect in term of confidentiality, integrity and authentication [35] as follow:

- Confidentiality: Ensure that data is accessed by authorized users only. Password and encryption algorithms can be used to provide a protection to the data in storage and during transmission.
- Integrity: Ensure that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. Checksums (CRCs) is considered one of the solutions to provide integrity through the protocol communication.
- Authentication: Verify the system entities to each other using mutual authentication protocol. Mutual authentication is required to prevent man-in-the-middle for User-to-Device (U2D), Device-to-Device (D2D), and Device to-Network (D2N).

Potential attacks on the RF system are then identified as in [36] as follows:

- Tracing: A tag/sensor response can be a constant serial number/sensor's ID enabling any unauthorized reader to identify the tag and track it in an unauthorized way. The countermeasure for this is that the tag response must appear as a random number and be refreshed frequently so the attacker will not be able to trace the tag [37].
- Cloning attack: An attacker with suitable equipment is able to clone any legitimate tags/sensor. Then, the attacker can communicate with a legitimate reader. The cloned tag/sensor claims to be genuine and will be accepted by the reader where, in fact, it is a fake one.
- Spoofing attack: An attacker with a suitable programmed portable reader might be able to read and record the data transmission from the tag/sensor to the reader. Then, the attacker emulates this data and retransmits it to the reader. On the reader side, data appears as a valid tag/sensor [38].
- Denial of Service (DoS) attack: This deals with the availability of the tag/sensor data and occurs when an attacker denies service to valid users. The usual method that can cause the DoS attacks is by flooding the network with illegitimate traffic, leaving the system unable to respond [39].
- Man in the Middle (MITM) attack: This is a form of active eavesdropping in which the attacker makes logical connections between two authorized parties and relays messages between them. The deceived two parties believe that they are talking directly to each other over a private connection. However, in fact, the attacker relays the messages between the authorized parties.
- Replay attack: Attackers can intercept and retransmit RF queries. However, using challenge-response authentication scheme or a sequence number that identifies each protocol session can improve the situation [40].

Actually, WSN and RFID faces security challenges, including key establishment, secrecy, authentication, privacy, robustness to denial-of-service attacks, reply attack, secure routing, and node capture. Therefore, there are some security aspects that the system designer should consider in order to build a secure system [41]. These aspects are as follows:

- Store critical data in the back end server (such as database) which must be in a secure environment.
- In order to prevent replay attacks security designers need to establish secret keys for the safe communication between the system components.
- To prevent spoofing designer need to use cryptography protocols. However, due to the limited computation power of both of the tag and sensor there is a need to find a lightweight encryption protocols.
- Attackers should not be able to use fake tags/ sensors that may provide wrong data. So, to prevent the cloning problem we must use shared stored secret between the system components, and use this secret in the authentication process; note that, this shared secret must be hard that attackers cannot predict.
- To prevent the DoS attack designers can depend on the network nature .When the jamming affects only a portion of the network, a jamming-resistant network could defeat the attack by detecting the jamming, mapping the affected region, then routing around the jammed area.

6. Scenario of Smart Chain Tracking

In order to achieve smart chain of tracking both of the RFID and WSN technologies are combined. The RFID tags are attached to the container (to identify the shipment) while the sensors (for the sensing ability such as environment temperature) are attached to the truck that will deliver the container to the end user. A reader also, is placed at the truck to gather shipment information and send it to the truck driver. The truck driver should be able to connect to the main central system that controls, gathers, and traces the shipment track during the way from the shipment provider to the end user. The EPC network consider as the main center that is used to connect the whole system from the source to the destination. The important of the shipment depend on the value of the shipment itself. For example if the shipment is types of weapons or gold then this shipment should have a secure tracking path. Intruder may try to know the shipment track and steal the shipment before it reaches its destination. Therefore, there is a need to add a security mechanism to both of the RFID and WSN to make it hard to the intruder to break. By adding a light cryptography protocol the shipment track can be invisible to the intruder and only the main center knows their shipment track. At the EPC network an additional component which is the security center is added. The security center can deal with encrypting and decrypting the messages coming from the truck to the main center or messages sent from the main center to the truck. Fig. 4 explains the Smart Chain Tracking System.

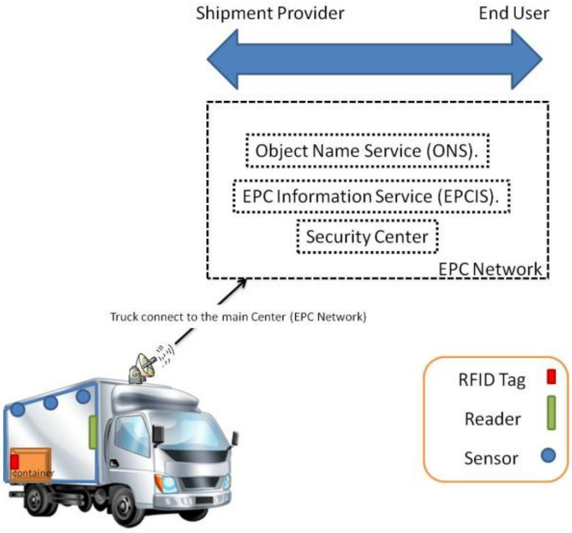
Shipment Provider
End User
Object Name Service (ONS).
EPC Information Service (EPCIS).
Security Center
EPC Network
Truck connect to the main Center (EPC Network)
RFID Tag
Reader
Sensor
container

Figure 4. Smart Chain Tracking System

7. Conclusion and Future work

The paper discussed the integration of the RFID and WSN technologies. There are many applications that need the integration of both technologies to enhance the system automation and convert the application into a smart system. Researchers try to build a standard system for both technologies so that the integration can be adopted easily. However, the integration system must be built with security aspects in mind. In this paper we tried to analyze the threats and attacks on the integrated technologies and highlighted some considerations that should be followed in building such a system in a secure manner. In the EPC network architecture that we suggest as basis for the integrated technologies the new adopted design can add a Security Center that deals with the key establishment, authentication, encryption and decryption of the messages between the tag/sensors and the reader or backend server. Our future work will continue exploring this research area and will try to build a secure smart chain tracking system. The project combines both of the RFID and WSN technologies that will be built in a secure way by adding our own mutual authentication protocol.

8. References

[1] Comments on EC Working Document 10107/05/EN WP 105, Developed by the RFID Experts Group of AIM Global, AIM Regional Support Centre – Europe, Middle East and Africa, Jan. 2005,http://www.aimglobal.org.

[2] V. Hunt, A. Puglia and M. Puglia, "RFID: A Guide to Radio Frequency Identification", Wiley Inderscience, Edition 1, April 10, 2007.

[3] M. Ward and R. van Kranenburg, "RFID: Frequency, standards, adoption and innovation", JISC Technology and Standards Watch, May 2006.

[4] Jae-Bong Yoo, Byung-Ki Kim, Ho-Min Jung, Taewan Gu, Chan-Young Park, Young-Woong Ko. “Design and Implementation of Safe & Intelligent Bridges System Based on ALE-Compliant RFID Middleware in USN”, 5th International Conference on Computer Science, Rome, Italy, Vol 2 No 2, pp 101-107, 2008.

[5] A. S. Voulodimos, C. Z. Patrikakis, A. B. Sideridis, V. A. Ntafis, E. M. Xylouri, “A complete farm management system based on animal identification using RFID technology”, Computers and Electronics in Agriculture, 2009.

[6] Valentin POPA, Cristina TURCU, Vasile GAITAN, Cornel TURCU, Remus PRODAN. “Optimizing Campus Access and Services Using RFID Solutions”, Proc. 8th International Conference on Development and Application Systems, pp. 228-233, Suceava, Romania, 2006.

[7] C. Goebel, C. Tribowski, O. Günther, R. Troeger, R. Nickerl, ”RFID in the Supply Chain: How to Obtain a Positive ROI - The Case of Gerry Weber”, Proc. 11th Int. Conference on Enterprise Information Systems (ICEIS 2009), Vol. Information Systems Analysis and Specification, pp. 95-102, Milan, Italy, 2009

[8] K. Werner, A. Schill, “Automatic Monitoring of Logistics Processes Using Distributed RFID based Event Data”, 3rd International Workshop on RFID Technology - Concepts, Applications, Challenges (IWRT 2009), Milan, Italy, 2009.

[9] M. Lewis, B. Sankaranarayanan,A. Rai, "RFID-Enabled Process Capabilities and Their Impacts on Healthcare Process Performance: A Multi-level Analysis," in European Conference on Information Systems, 2009.

[10] Fennani, and H. Hamam, “An Optimized RFID-Based Academic Library”, 2nd Int. Conference on Sensor technologies and Applications, pp. 44-48, 2008.

[11] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “A survey on wireless sensor network”, IEEE Communication Magazine, Vol. 40, Aug 2002, pp. 102-114

[12] D. Cutler, D. Estrin, M. Srivastva, ”Overview of sensor networks”, IEEE Computer, Vol.37, no.8, pp. 41-49, 2004

[13] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, “A Survey on Sensor Networks”, IEEE Communication Magazine, vol. 40, no. 8, Aug. 2002, pp.102-114.

[14] H. labiod, H. afifi, c. de santis,”Wi-Fi, Bluetooth, Zigbee and Wimax” springer, 2007.

[15] Md. Abdullah-al Mamun, Yuji koi, Naoshi Nakaya, Goutam Chakraborty: a novel integrated wireless sensor network architecture for disaster prevention,international journal on smart sensing and intelligent systems, Vol. 2, NO. 2, June 2009.

[16] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, and J.A. Stankovic. An Advanced Wireless Sensor Network for Health Monitoring. In Proc. of the Transdisciplinary Conf. on Distributed Diagnosis and Home Healthcare (D2H2), April 2006.

[17] Varchola, M., Drutarovský, M.: ZigBee Based Home Automation Wireless Sensor Network. Acta Electrotechnica et informatica, No.4, Vol. 7, 2007, pp. 60-67.

[18] Wenjie Chen, Lifeng Chen, Zhanglong Chen, Shiliang Tu, "WITS: A Wireless Sensor Network for Intelligent Transportation System," imsccs, vol. 2, pp.635-641, 2006 First International Multi-Symposiums on Computer and Computational Sciences, 2006.

[19] Mason, A. I. Al-Shamma'a, and A. Shaw, "RFID and Wireless Sensor Network Integration for Intelligent Asset Tracking Systems," presented at the 2nd General Engineering Annual Research Symposium (GARS-2006), Liverpool John Moores University, Liverpool, UK, 2006.

[20] Rolf Clauberg,RFID and Sensor Networks,RFID Workshop, University of St. Gallen, Switzerland, Sept. 27, 2004.

[21] R. Want, “Enabling ubiquitous sensing with RFID”, IEEE computer, Vol.37, no.4, pp 84-86, 2004

[22] L.T. Sanchez, T. Lopez, H. Daeyoung, ‘Wireless sensor network and RFID integration for context aware services”, Tech. Report, Auto-ID Labs white paper series, 2008.

[23] C. Englund, H. Wallin, “RFID in wireless sensor network”, Tech. Report, Dept. of Signals & systems, Chalmers Univ. of Technology, Sweden, 2004.

[24] Aikaterini Mitrokotsa and Christos Douligeris, “Integrated RFID and Sensor Networks: Architectures and Applications,” RFID and Sensor Networks, pp. 511-536, 22 June 2009.

[25] Xin Shi, Shijuan Su, Qingyu Xiong, “The integration of Wireless Sensor Networks and RFID for pervasive computing”, 5th Int. Conference Computer Sciences and Convergence Information Technology, pp. 67-72, 10 February 2011.

[26] Yang Xiao, Xuemin Shen, Bo Sun, and Lin Cai, Security and Privacy in RFID and Applications in Telemedicine, Communication Magazine, IEEE, Vol. 44, Issue 4, pp. 64-72, April 2006.

[27] B. Lee, H. Kim, "Privacy Management for Medical Service Application Using Mobile Phone Collaborated with RFID Reader”, 3rd International IEEE Conference on Signal-Image Technologies and Internet-Based System, pp.1053-1057, 2007.

[28] B. Lee and H. Kim. “Ubiquitous RFID based Medical Application and the Security Architecture in Smart Hospitals”, International Conference on Convergence Information Technology, 2007

[29] A.Carullo, S. Corbellini, M. Parvis, L. Reyneri, A. Vallan, “A Measuring System for the Assurance of the Cold-Chain Integrity”, IEEE Instrumentation and Measurement, Vol 58, pp. 1405-1411, May 2009.

[30] B. B. Bravo, J. C. Fernández, M. M. Barrera, J. R. Sánchez, "Implementation of RFID tags in food containers in catering business.", 2010 European Workshop on Smart Objects: Systems, Technologies and Applications, pp. 1-6, 15-16 June 2010.

[31] EPCglobal Ratified Specification, “The EPCglobal Architecture Framework,” 15 December 2010.

[32] T. Staake, F. Thiesse, and E. Fleisch, "Extending the EPC network: the potential of RFID in anti-counterfeiting", in Proc. SAC, 2005, pp.1607-1612.

[33] Jongwoo Sung, Tomas L. Sanchez, Daeyoung Kim, "EPC Sensor Network for RFID and USN Integrated Infrastructure", 5th Annual IEEE International Conference on Pervasive Computing and Communications, New York, USA, Mar 19-23, 2007.

[34] Weixin Wang; Jongwoo Sung; Daeyoung Kim, “Complex Event Processing in EPC Sensor Network Middleware for Both RFID and WSN”, Proc. 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC), 2008 , pp.165–169, 5-7 May, 2008.

[35] C.Y. Yeun, E.K. Lua and J. Crowcroft, “Security for Emerging Ubiquitous Networks”, In Proceeding of the IEEE 62ND Semiannual Vehicular Technology Conference, Dallas, Texas, USA, September 25-28, 2005, Vol. 2, pp. 1242-1248.

[36] Mitrokotsa, M. R. Rieback and A. S. Tanenbaum, "Classification of RFID Attacks". In Proceedings of IWRT'2008. pp. 73-86, 2008.

[37] M. Burmester and B. de Medeiros, "RFID Security, Countermeasures and Challenge", 5th RFID Academic Convocation, The RFID Journal Conference, Orlando, April 30 - May 2, 2007.

[38] B. Moore, "RFID: Cloning vs. Spoofing", 2006. www.m-indya.com/shownews.php?newsid=1524

[39] Householder, A. Manion, L. Pesante, G. M. Weaver and R. Thomas, "Managing the Threat of Denial-of-Service Attacks", CERT, v10.0, October, 2001, http://www.cert.org/archive/pdf/Managing_DoS.pdf,

[40] M.R. Rieback, B. Crispo, A.S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?", PerCom 2006, pp.169-179, 2006.

[41] Adrian Perrig, John A. Stankovic, and David Wagner. “Security in wireless sensor networks”, Comm. ACM, 47(6):53-57, 2004.