Study of recent development about privacy and security of the Internet of Things

Hailong Feng
School of Electronic and Information Engineering
Beijing Jiaotong University
Beijing ,P.R.China
e-mail:fenghailong008@126.com

Wenxiu Fu
School of Electronic and Information Engineering
Beijing Jiaotong University
Beijing ,P.R.China
e-mail:wxfu@bjtu.edu.cn

***Abstract*—This paper depicts the current situation of the development of the Internet of Things(IoT). RFID system is vulnerable to various attacks, because there is no physical or visible contact in its communication process. The research on security and privacy domain also increasingly causes the attention of academia. And this paper is mainly underlined that security and privacy issues exist ubiquitously,these problems are not completely solved until now. In succession , different approaches recently been proposed to address security and privacy issues are discussed and analysised specifically in the world of the Internet of Things. Meanwhile, the challenges and future trends of the IoT are also mentioned.**

Keywords- RFID; IoT ; Privacy; Security

I. INTRODUCTION

Radio frequency identification (RFID) is a wireless automatic identification technology, which is used to identify or authenticate remote objects or persons, through a radio frequency channel using devices called RFID readers and RFID tags. RFID technology has numerous advantages such as contactless, speediness, multi-objects identification, etc. RFID technology is one of the most promising technologies of this decade , develops fast with potentially wide application in the fields of traffic,industries, transportation, purchasing, distribution logistics,security, anticounterfeiting, etc.RFID systems fundamentally consist of three elements: RFID tags, RFID readers and a back-end server. Fig. 1 shows a typical RFID system.

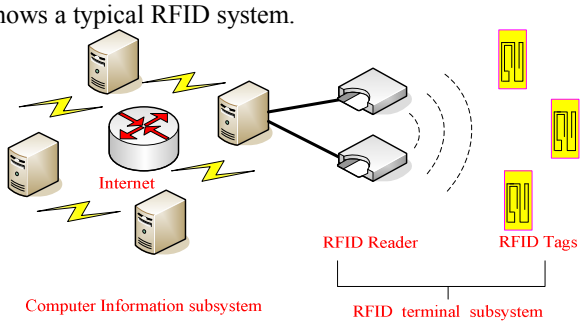

Figure 1. Typical RFID system

The concept of Internet of Things (IoT) was developed by the MIT Auto-ID Center in 2001,and they conceived a networked physical world[1],that is a world in which all electronic devices are networked to form a global intelligent infrastructure and every object is electronically tagged, so as to enable ubiquitous and automated identification using that infrastructure. The internet reports 2005 "The Internet of Things " of the ITU(International Telecommunication Union) described that everything might soon be in communications range, heralding the dawn of a new era; one in which today's Internet gives way to tomorrow's the IOT [2].

IoT will pervade people everyday's life in future and could be used to improve quality of their users' lives. However ,from the other side, such systems by collecting information about people's daily activities can easily violate individual privacy. Because a RFID tag replies its unique ID to the request of any reader through wireless communication, it is vulnerable to attacks on security or privacy. As RFID tags' non-selective response to all readers' queries, items identified with tags may leak sensitive information,on which adversary can achieve their trace goals rely.The track also be said against the location privacy.Besides privacy and traceability ,the two major security threats, RFID systems are also subject to physical attacks, denial of service attacks, cheat tags,eavesdropping and communication flow analysis and other security threats. Without the appropriate control solutions, attackers can perform unauthorized tag reading.

Therefore, RFID systems must be able to resist all forms of attacks. However ,until recently the developers of ubiquitous applications have focused mostly on functionality what can potentially limit usability and acceptance of such applications by potential users[3], lots of the security threats and violation attempts exist in RFID systems which do not appear robust enough to address. Thus the privacy concerns become a increasingly critical issue. In this paper, we will systematically summarize and analyze the existing security methods and mechanisms used in the IoT.

The rest of the paper is organized according to the following outline. Section 2 introduces the background of the IoT;Section 3 makes a study about the security and privacy of IoT ,including security strategy recently proposed for security of the IoT;while the section 4 explains the challenges remain and future trends for IoT's development; Finally, in section 5, we make concluding remarks.

II. THE INTERNET OF THINGS

A. *The Architecture of IoT*

The structure of the Internet of Things is shown in Fig. 2. In the system of the Internet of Things [4], each object has

978-0-7695-4224-9/10 $26.00 © 2010 IEEE
DOI 10.1109/WISM.2010.179

been given a unique RFID code, which is stored in RFID tag. Meanwhile, the detailed information and attributes for each object are stored in the RFID Information Service (RFID-IS) server. When reader reads the tag, RFID code will be sent to RFID Middleware(RFID-MW).Afterward,RFID-MW sends an inquiry command to the RFID Naming Service(RFID-NS) server through the Internet. After RFID-NS server receives inquiries, it searches the correlative address information according to the rules (like the DNS function in Internet). And then, it leads RFID-MW to access the RFID-IS server with the detailed information of things. After RFID-IS server receives inquiry command, it will send the detailed information in the form of a homepage to RFID-MW, and the inquirer will obtain the information about the object.

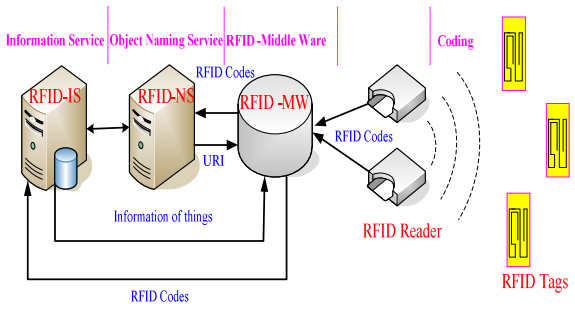

Figure 2. The architecture of the IoT

B. The Development of the IoT

*1) Current Development of the IoT in developed countries and regions:*In recent years, the world's major developed countries and regions have thrown out the information strategy connected with IoT. Such as, in 2004, Japan proposed "U-Japan" plan; In the end of 2008, the corporation IBM proposed "smart earth" strategy toward to the U.S. Government; in June 2009, the EU launched an campaign named " Plan of Action about IoT",etc. [5].

2) Current Development of the IoT in China: China deployed early in the field of IoT, e.g., Chinese Academy of Sciences (CAS)started the research on sensor network at 10 years ago, the CAS Shanghai Institute for Microsystem and Information Technology, Nanjing University of Aeronautics and Astronautics, Northwestern Polytechnical University and other research units,are currently stepping up researching on technology of IoT. By 2020, China will plan with funds of 3.86 trillion RMB for the research of IoT[5].

III. STUDY FOR SECURITY OF THE IOT

A. General Security Mechanism for the IoT

Nowadays, in literature, various methods are proposed to mitigate privacy and security problems in RFID systems. These RFID security mechanisms mainly are divided into three categories: physical methods, anti-collision algorithm mechanism and encryption authentication mechanism.

1) Physical security mechanism: using physical methods to protect the safety of RFID Tags. The main methods are: electrostatic shielding[6], Blocker Tag[7], active jamming[7], Kill command mechanism[8], etc. These methods mainly are used in the low-cost Tags, because these tags have some strict restrictions to cost, it is difficult to use a complex encryption system to communicate with the Tag reader safely. In view of drawback [9]of the physical security mechanism, in recent RFID system, researchers put forward a number of security authentication mechanisms based on cryptography.

2) Anti-collision algorithm mechanism: Currently, the problem of RFID collision is divided into two kinds:tag collision and reader collision[10]. When a large number of electronic tags get acess to reading area, the individual reader often makes mistakes, such as missing data,etc., a collision occurs among tags called tag collision;To enhance the rate and accuracy of reading, considerable readers are needed to arrange, as a result of this , generating a dense environment composited of a large number of tags and readers. In this environment, collision will occur between tags and readers, readers and readers , the two kinds of collisions are both called reader collision. Here's what solutions has been proposed for the two kinds of collisions:

a) Tag Anti-collision Algorithm: Tag anti-collision algorithm can be divided into deterministic methods and probabilistic methods. The former is based on tree structure, the basic principle is to divide collision group into subgroups until all tags are readed .Such as, the generalized binary tree protocol (GBT)[11], binary tree algorithm based on parallel binary splitting (PBS) technique[12];The probabilistic methods allow tags to respond at different times in order to reduce the probability of collision,and it mainly refer to the ALOHA algorithm and its variants, such as, a dynamic framed slotted ALOHA algorithm based on bayesian estimation is proposed in[13];In order to address problem of multiaccess communication and power dissipation in RFID system, A New Energy-Aware Scheme Based on ALOHA is proposed in[14],etc.

b) Reader Anti-collision Algorithm : Tag collision problem has been extensively studied. However, studies internationally on RFID reader anti-collision algorithm are not very adequate. With the concept of the Internet of Things was proposed ,the establishment of large-scale RFID network in which readers work collaboratively is imperative. Anti-collision algorithm published was divided into scheduling-based and coverage-based solutions[15] [16]. The core idea of coverage-based anti-collision algorithm is to reduce the coverage overlap between the readers in order to reduce collisions between readers. But,this kind of approach needs a central node to calculate the distance between every two readers, which will increase the complexity of realization and cost of the system[17].Coverage-based anti-collision algorithm are mainly related to LLCR [18] and w-LCR [19], such algorithms adjust the communication range of readers by power adjustment of reader.Differently ,the core idea of

scheduling-based anti-collision algorithm is to prevent the reader sends simultaneously a signal to the tag avoiding the collision.Since the RFID reader collision problem has been proposed, such algorithm has been the mainstream of the anti-collision algorithm.Anti-collision algorithm based on scheduling mainly includes:colorwave[20],enhanced colorwave[21],Pulse algorithm[22], Improved Pulse Protocol with Slot Occupied Probability[17], DiCa (Distributed Tag Access with Collision-Avoidance) algorithm [23], HiQ (Hierarchical Q-Learning Algorithm) [24]and SA (Simulated Annealing Algorithm) [25], MRC (Main Reader Control) algorithm[26], CC-RFID(Central Cooperator) scheme[16],etc. In short, various algorithms have their advantages and disadvantages [10] [15], for example, even though tags anti-collision algorithm has been extensively studied, most of them have some shortcomings ,such as long delay, the large energy consumption etc. Meanwhile ,the deficiencies- low efficiency of reader anti-collision algorithm still exist, so anti-collision problem will remain a hot issue in RFID's development and process of its application, different applications should aim to select a different algorithm.

3) Encryption& Authentication Protocol mechanism: using sophisticated encryption schemes and mechanisms to design and implement RFID security protocols which meet requirements of RFID system. This has become another hot research on RFID security. The current security protocols in discussion are: RFID private authentication protocol – RWP(based on the random walk concept)[27] , AFMAP(Anonymous Forward-Secure Mutual Authentication Protocols)[28], Ultralightweight RFID Mutual Authentication Protocols[29], Mutual authentication protocol based on tag ID number updating [30]etc. As a fundamental tool in communication security,cryptography can be used to provide data authentication and confidentiality.But unfortunately, for most of the existing RFID protocols, there are various defects[9][31]. Standard cryptographic algorithms need more storage and computation resources than what are available in RFID tags to be carried out. Therefore, a protocol designed for RFID authentication must consider not only security and privacy threats but also storage and computation capabilities of RFID tags. In general terms, there are two types of cryptographic solutions available depending on whether we use symmetric (secret-key) cryptography or asymmetric (public-key) cryptography.

Digital signatures are an important tool for data and device authentication. Digital signatures and hash functions already play an important role in providing data security to communication applications.O'Neill, M.and Robshaw, M.J.B. [32]proposed a low-cost GPS digital signature architecture, which combined an optimised GPS algorithm design and an optimised SHA-1 design, is proposed for low-cost RFID tags. The proposed architecture can be used for device authentication to prevent tag cloning and to provide data authentication to prevent transmission forgery.

In recent years ,the research of mobile RFID systems has been concerned increasely. Taking into account computing load to the low cost tag and sufficient protection to the information privacy ,designing RFID authentication schemes which are suitable to use in mobile RFID environment is not a simple task.Ming Hour Yang and Jia-Ning Luo[33] proposed a lightweight authentication protocol in mobile RFID and complied with EPC Class-1 Gen-2 norms.The scheme was claimed that it effectively achieved forward security with preventing replay,Man-in-the-Middle(MITM),eavesdropping, and counterfeit tag attacks, and ensured tag data and location privacy in authentication stage under the network infrastructure of mobile RFID, which also ensured the tag owners eliminate being traced of their location during the authentication.

B. Security Strategy based on architecture for Privacy and Security of the IOT

Besides the three mechanism — physical methods，anti-collision algorithm and encryption authentication, recently, the academia has raised many mechanism based on architecture to solve the security and privacy problem of the IoT. Here enumerates a few of typical ways to explain it.

1) HIP-Tags Architecture Implementation for IoT: Security and privacy issues revolve around the capabilities of RFID Architecture, to conciliate location and mobility management, by extension, to compensate for the existing weaknesses between the Internet Protocol (IP) addresses and Domain Name Service (DNS) names.T2TIT (The Things To Things in the Internet of Things, a project is funded by the French National Research Agency ,aims at defining and standardizing a highly secure networking infrastructure) introduces a new type of RFID, which communicates with the Internet thanks to the Host Identity Protocol (HIP), recently defined by the IETF[34].P.Urien, et al. first introduced the HIP Tag model[35]. Meanwhile,they proposed a HIP Address Translation (HAT) mechanism and the privacy protocol adapted to their HIP tags model.And, they discuss the portal architecture and proposed a middleware to handle HIP Tags.In the following year, P.Urien, et al. [36]presented detailed architecture and specifications of new HIP-tags that ensure privacy while enabling things to things communications.

2) Self Managed Security Cell—a security model for the IoT and Services: The concept of the Internet of Things and Services (IoT&S) is based on the possibility of seamless integration of physical objects such as sensors or home appliances and services, which can be loosely defined as a network interface that exposes a piece of functionality.Pierre de Leusse et al. focus on the need to define and comprehend the requirements that have risen with the IoT&S in order to model a generic architectural

framework to secure resources.They proposed an architectural model of Self Managed Security Cell[37], which leveraged on current knowledge in large scale security systems, information management and autonomous systems. This model underlined the need for interoperability, decentralisation, automation and contextualisation in modern security systems. An example of a potential application of this architecture had been presented and defined in the SOI-SSG（Service Oriented Infrastructure-Service Security Gateway）.

3) Mobile Proxy-a novel RFID privacy protection mechanism: Eunah Kim et al.proposed the concept of mobile proxy to protect consumer privacy using a mobile phone[38]. When a consumer carries RFID tags embedded in personal items in his wireless PAN (Personal Area Network), the main controller of the PAN, the mobile phone can administrate tags' data, monitor the query of nearby readers, and mediate the communications between tags and readers with specified consumer's privacy policies easily. Refering this mobile proxy as a PPPH (PAN Privacy Protection in Hand).The Mobile phone equipped with RFID reader module regulate tags within wireless PAN range and communicates with nearby RFID readers on behalf of basic tags. Existing mobile infrastructures can be used for storing RFID tags' data in the back-end database systems ,which are normally used in RFID system.Eunah Kim et al. implemented a prototype of PPPH which can be applicable in recent high performance smart phone .

4) LKC-privacy and its anonymization algorithm –a protection method of RFID data privacy: A comprehensive privacy-preserving information system must protect its data throughout its lifecycle, from data collection to data analysis. Most previous work on privacy-preserving RFID technology, such as EPC re-encryption and killing tags, focused on the threats caused by the physical RFID tags in the data collection phase, but these techniques cannot address the privacy threats in the data publishing phase, when a large volume of RFID data is released to a third party. In view of this situation,Fung, B.et al. defined a new privacy model[39], called LKC-privacy for anonymizing high-dimensional RFID data. They developed an anonymization algorithm to address the special challenges on RFID data, and evaluated its performance in terms of data quality and efficiency. The principle was to transform the underlying raw object-specific RFID data into a version that was immunized against privacy attacks.

IV. CHALLENGES AND FUTURE TRENDS FOR THE IOT'S DEVELOPMENT

A. Challenges of the IoT

The incredible amount of information captured by a trillion RFID tags will have a tremendous impact on our lives. The relevant researches related to the IOT are still in their infancy, and most of them just use the Internet's existing technology, so they cannot resolve some new problems accompanying with IoT's development. For example ,future applications of RFID technology will require creation of complex reader networks. Readers used today are not suitable for this task due to lack of interoperability. Absence of reader-to-computer interaction standards is an obvious drawback nowadays[40].

The fact that tags had only modest computational capabilities,combined with the need for low prices, presented a challenging dilemma that gone beyond the well-studied problems of traditional authentication and access management.Spiekermann S.and Evdokimov S. [41]categorized,summarized, and critically discussed advanced 218 papers research in the domain of privacy enhancing technologies (PETs) aimed at preventing unauthorized access to RFID tags.The author divide the end-user RFID PETs described in the 97 papers(44 percent of the total) into five categories.Their analysis of the five privacy management models showed that none is truly optimal. Each proposal involves trade-offs concerning security levels, tag cost, key management complexity, and user transaction cost. Furthermore, each solution achieves a different level of user control[41].

B. Future Trends of the IoT

In the report "Internet of Things in 2020:A Roadmap for the future,"[42], EPOSS(European Technology Platform on Smart Systems) analysised and forecasted,the Internet of Things will experience four stages of development in the future : by 2010, RFID would be widely used in logistics, retail and pharmaceutical sector; all objects would be interconnected with together globally from 2010 to 2015; the IoT would go in the"semi-intelligent" world from 2015 ~ 2020; after 2020, all objects would be"intelligent"worldwide . There is no doubt that the objectives which should be implemented by 2010 have been achieved successfully.

V. CONCLUSION

In this paper,we make a simple presentation about the Internet of Things ,then we discuss about security mechanisms which had been already proposed recently for the IoT. At the same time, we also point out that the challenges for IoT's development remain existing.We have ample reason to believe,in the future, research on the Internet of Things will remain a hot issue, and a lot of knotty problems are waiting for researchers to deal with.

REFERENCES

[1] Auto-ID Center . http://www.autoidlabs.org.

[2] "The Internet of Things,"ITU Internet Reports, Geneva, Nov.2005.

[3] Vladimir Oleshchuk, "Internet of Things and Privacy Preserving Tech nologies,"1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electro nic Systems Technology,Aalborg , IEEE Press,May 2009,pp.336-340, doi: 10.1109/WIRELESSVITAE.2009.5172470.

[4] EPC Global. http://www.epcglobalinc.org.

[5] "2010-2013 report: panoramic investigate and investment strategy stu dy about Internet of Things in China,"http://www.askci.com,Nov.200 9. (In Chinese)

[6] Sanjay E.Sarma,Stephen A.Weis and Daiel W.Engels,“Radio-frequency identification:Secure risks and challenges,”RSA Laboratories Cryptobytes,vol. 6, Jun.2003, pp.2-9.

[7] Juels A.,Rivest R.L.,Szydlo M., “The blocker tag:Selective blocking of RFID tags for consumer Privacy,” Proceedings of the 10th ACM Conference on Computer and Communications Security(CCS 2003) Washington DC,USA,2003,pp.103-111.

[8] Weis S.A.,Sarma S.E.,Rivest R.L.,Engels D.W., “Security and privacy aspects of low-cost radio frequency identification systems,” SECURITY IN PERVASIVE COMPUTING, vol. 2802, 2004, pp. 20l-212.

[9] Yongbin Zhou,Dengguo Feng, “Design and Analysis of RFID Security Protocol,”Chinese journal of computers, vol.29 ,no.4 , Apr.2006,pp. 581-589.(In Chinese)

[10] Bingyun Lv,Jianxia Pan,Qi Ma,Zihua Xiao,“Research Progress and Application of RFID anti-collision algorithm,”Telecommunication Engineering,China,vo1.48 , no.7 , Jul.2008,pp.124-128.(In Chinese)

[11] Yuan-Cheng Lai, Ling-Yen Hsiao,“General binary tree protocol for coping with the capture effect in RFID tag identificationpp,” Communications Letters, IEEE ,vol. 14, Mar. 2010, pp. 208- 210,doi: 10.1109/LCOMM.2010.03.092208

[12] Mohammed, U.S. ,Salah, M., “Parallel binary tree splitting protocol for tag anti-collision in RFID systems,” 2009 4th International Design and Test Workshop (IDT), Riyadh,Nov.2009,pp.1-6,doi: 10.1109/IDT.2009.5404155

[13] Qiaoling Tong,Xuecheng Zou,Hengqing Tong,“Dynamic Framed Slotted ALOHA Algorithm Based on Bayesian Estimation in RFID System,” 2009 WRI World Congress on Computer Science and Information Engineering(CSIE), Los Angeles, CA,vol. 1, Apr. 2009, pp. 384 - 388, doi: 10.1109/CSIE.2009.248

[14] Kaixing Wu,Yuankun Liu , “A New Energy-Aware Scheme for RFID System Based on ALOHA,”The second International Conference on Future Networks(ICFN 10), Sanya,China, IEEE Press, Jan.2010,pp.149-152,.doi: 10.1109/ICFN.2010.29

[15] Leiyong Guo,Hongzhou Tan,Shouping Gao,Xiaomei Guo , “study and classification of reader anti-collision algorithm for RFID system,” Chinese Computer Technology and Development,vo1.19,no.9, Sep.2009,pp.13-17.(In Chinese)

[16] D. Wang, J. W. Wang, and Y. P. Zhao, “A novel solution to the reader collision problem in RFID system,” Proc. IEEE Wireless Communications,Networking and Mobile Computing,(WiCOM 06),Sep. 2006,pp.1-4,doi: 10.1109/WiCOM.2006.340

[17] InChan Song , SungHyun Hong ,KyungHi Chang,“An Improved Reader Anti-collision Algorithm based on Pulse Protocol with Slot Occupied Probability in Dense Reader Mode,” IEEE 69th Vehicular Technology Conference, Barcelona, Apr.2009,pp.1-5,doi: 10.1109/VETECS.2009.5073385

[18] Kim J,Lee W,Yu J,et al. “Effect of localized optimal clustering for reader anti-collision in RFID networks:fairness aspects to the readers,”IEEE International Conference on Computer Communications and Networks, Oct.2005,pp.497-502, doi:10.1109/ICCCN.2005.1523923

[19] Kim J,Lee W,Jung J,et a1.“Weighted Localized Clustering:A Coverage-Aware Reader Collision Arbitration Protocol in RFID Networks,” EMBEDDED SOFTWARE AND SYSTEMS, PROCEEDINGS, vol. 3820, Dec.2005, pp.542-553.

[20] Waldrop J,Engels D W,Sanna S E, “Colorwave:An anticolison algorithm for the reader collision problem,” IEEE International Conference on Communications(ICC 03), New Orleans,Louisiana USA, vol..2,May.2003,pp.1206-1210,doi: 10.1109/ICC.2003.1204562

[21] S. R. Lee and C. W. Lee, “An enhanced colorwave reader anti-collision algorithm in RFID system,” Journal of the Institute of Electronics Engineers of Korea, vol. 43, no. 2, Aug. 2006, pp. 27-37.

[22] Shailesh M Birari,Sridhar Iyer, “PULSE:A MAC Protocol for RFID Networks,” Lect. Notes Comput. Sci.,vol.3823, Dec. 2005，pp.1036-1046

[23] Hwang K,Kim K,Eom D, “DiCa:Distributed Tag Access with Collision-Avoidance Among Mobile RFID Readers,” Lect. Notes Comput. Sci.,vol.4097, Aug.2006, pp.413-422.

[24] Ho Julius,Daniel W Engels,Sanjay E Sarma, “HiQ:A Hierarchical Q-Learning Algorithm to Solve the Reader Collision Problem,” Proceedings of the International Symposium on Applications and the Internet Workshops, vol.2006, Jan. 2006, pp. 88-91.

[25] Chun-Fu Lin,Frank Yeong-Sung Lin,“A Simulated Annealing Algorithm for RFID Reader Networks,”IEEE Wireless Communications and Networking Conference (WCNC 07), Mar.2007, pp. 1669 -1672 .

[26] D. H. Ahn, H. G. Yang, S. H. Yang, and Y. S. Kim, "Multiple Access Protocol of RFID Reader" Korean Information and Communications Society Magazine, vol. 24, no. 5, May 2007, pp. 124-134.

[27] Qingsong Yao,Yong Qi, Jinsong Han ,Jizhong Zhao,Xiangyang Li,Yunhao Liu , “Randomizing RFID private authentication,” IEEE International Conference on Pervasive Computing and Communications, Mar.2009, pp.1-10,doi: 10.1109/PERCOM.2009.4912773

[28] Sadighian,A., Jalili, R.,“AFMAP:Anonymous Forward-Secure Mutual Authentication Protocols for RFID Systems,”Third International Conference on Emerging Security Information, Systems and Technologies, Jun.2009, pp.31-36, doi: 10.1109/SECURWARE.2009.12.

[29] Lee Y.C. , Hsieh Y.C. ,You P.S. , Chen T.C., “A New Ultralightweight RFID Protocol with Mutual Authentication,” International Conference on Information Engineering(ICIE 09), Taiyuan, China,vol.2, Jul. 2009, pp.58- 61,doi: 10.1109/ICIE.2009.24.

[30] Yonghao Gu,Weiming Wu, “Mutual authentication protocol based on tag ID number updating for low-cost RFID,” IEEE International Conference on Network Infrastructure and Digital Content(ICNIDC 09), Nov. 2009. pp. 548 – 551,doi: 10.1109/ICNIDC.2009.5360812.

[31] Cagatay Karabat , “A Novel Secure RFID System to Ensure Privacy,” 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing(IIH-MSP 09), Kyoto ,Sep. 2009, pp.442-445,doi: 10.1109/IIH-MSP.2009.120

[32] O'Neill M. ,Robshaw M.J.B., “Low-cost digital signature architecture suitable for radio frequency identification tags,”Computers & Digital Techniques, IET ,vol.4, Jan.2010, pp. 14-26.

[33] Ming Hour Yang,Jia-Ning Luo, “Authentication Protocol in Mobile RFID Network,” Fourth International Conference on Systems(ICONS 09), Guadeloupe,Mar.2009, pp.108-113,doi: 10.1109/ICONS.2009.9.

[34] P.Urien, H.Chabanne,et al. “HIP-based RFID Networking Architecture,” IFIP International Conference on Wireless and Optical Communications Networks, Jul.2007, pp.1-5,doi:10.1109/WOCN.2007.4284140.

[35] P.Urien, et al. “HIP-Tags, a new paradigm for the Internet Of Things,” WirelessDays,1st IFIP, Dubai ,Nov.2008,pp.1-5,doi: 10.1109/WD.2008.4812927.

[36] P. Urien, S. Elrharbi,et al. “HIP-Tags architecture implementation for the Internet of Things,” First Asian Himalayas International Conference on Internet,Nov.2009,pp.1-5,doi: 10.1109/AHICI.2009.5340263

[37] Pierre de Leusse, Panos Periorellis, Theo Dimitrakos, Srijith K. Nair, “Self Managed Security Cell, a security model for the Internet of Things and Services,”2009 First International Conference on Advances in Future Internet, Jun. 2009. pp.47-52, doi: 10.1109/AFIN.2009.15.

[38] Eunah Kim, Taekyoung Kwon, and Jeong Hyun Yi,“A Study of Mobile Proxy for Privacy Enhancement,” 2010 Digest of Technical Papers International Conference on Consumer Electronics(ICCE 10), Jan. 2010, pp.177-178,doi: 10.1109/ICCE.2010.5418783.

[39] Fung B.,Al-Hussaeni K.,Cao M., “Preserving RFID Data Privacy,” IEEE International Conference on RFID , Orlando, FL, Apr. 2009, pp. 200-207,doi: 10.1109/RFID.2009.4911184

[40] Vladimir Dashevsky,Boris Sokolov, “New concept of RFID reader networks structure:hardware and software architecture,” International Conference on Ultra Modern Telecommunications & Workshops, St. Petersburg ,Oct.2009, pp.1-4, doi: 10.1109/ICUMT.2009.5345332.

[41] Spiekermann S.,Evdokimov S.,“Critical RFID Privacy-Enhancing Technologies,” Security & Privacy, IEEE, vol.7, 2009, pp.56-62 , doi: 10.1109/MSP.2009.31

[42] EPoSS（European Technology Platform on Smart Systems） report: “Internet of Things in 2020:A Roadmap for the future,” http://www.smart-systems-integration.org.Sep. 2008.