Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 2, February : 2023

RFID MUTUAL AUTHENTICATION PROTOCOLWITH HIGH POWER AND LOW DENSENESS

S. SANDHYA, Assistant professor, Electronics and Communication Engineering, Anubose institute of Technology, Palvancha, Telangana, India.

D. SWECHA, Assistant professor, Electronics and Communication Engineering, Anubose institute of Technology, Palvancha, Telangana, India.

R. SATHEESH, Assistant professor, Electronics and Communication Engineering, Anubose institute of Technology, Palvancha, Telangana, India.

M. VARALAKSHMI, Assistant professor, Electronics and Communication Engineering, Anubose institute of Technology, Palvancha, Telangana, India.

Abstract

This project outlines the specifications for the reader-commandedfunctionality and radio frequency communication interface for an Auto-ID Center Class I Radio Frequency Identification (RFID) tag operating in the 8.6GHz– 9.3GHz frequency band. During the communication process, a Class I tag is solely intended to transmit its unique identifier and any other information necessary to retrieve it. The proposal outlines a customized acceptable security framework designed with RFID applications in mind. In this chapter, the gated driver tree concept is described as a way to save energy. We arrive at a model thatensures good security, privacy, and availability qualities while allowing the creation of workable RFID protocols by applying setup, communication, and concurrency assumptions particular to RFID. The deployment model used by the framework is modular, making it ideal for ubiquity applications.

1. Introduction

Radio Frequency Identification (RFID) is an automatic identification system, relying on storing and remotely retrieving data about objects we want to manage using devices called “RFID tag”. In the near future, RFID technology is expected to play an important role for object identification as a ubiquitous infrastructure. RFID technology is one of next generation technologies which is mainly used to identify massive objects and will be a substitution for the existing optical barcode system in the near future. The micro-chip equipped on has unique identification information and is applicable for various field such as animal tracking, supply chain management, inventory control, etc. Some widespread and commonly known applications of RFID are identification, tracking and real-time monitoring. RFID can provide real-time supply on location and status of goods. The ability to identify and track assets is critical for a retail store, a whole sale distributor, a manufacturer, or a hospital.

2. Related work

According to R. Want [1] Radio frequency identification has attracted considerable press attention in recent years, and for good reasons: RFID not only replaces traditional barcode technology, it also provides additional features and removes boundaries that limited the use of previous alternatives.

According to T Dimitrio [2] Radio Frequency Identification (RFID) is a method of remotely storing and retrieving data using small and inexpensive devices called RFID tags. Products labeled with such tags can be scanned efficiently using readers that do not require line-of-sight. This form of identification, often seen as a replacement of barcode technology, can lead to improved logistics, efficient inventory management, and ultimately better customer service.

According to S. Han [3] an efficient localization scheme for an indoors mobile robot using Radio-Frequency Identification (RFID) systems. The mobile robot carries an RFID reader at the bottom of the chassis, which reads the RFID tags on the floor to localize the mobile robot. Each of the RFID tags stores its own absolute position, which is used to calculate the position, orientation, and velocity of the mobile robot. However, a localization system based on RFID technology inevitably suffers from an estimation error. In this paper, a new triangular pattern of arranging the RFID tags on the floor has been proposed to reduce the estimation error of the conventional square pattern. In addition, the motion-continuity property of the differential-driving mobile robot has been utilized to improve the localization accuracy of the mobile robot. According to the conventional approach, two readers are necessary to identify the orientation of the mobile robot. Therefore, this new approach, based on the motion-continuity property of the differential-driving mobile robot, provides a cheap and fast estimation of the orientation. The proposed algorithms used to raise the accuracy of the robot localization are successfully verified through experiments.

According to Class 1 Generation2 [4]The International Standards Organization (ISO) and EPCglobal are two organizations that work together to approve standards and

protocols in order to provide universal specifications for RFID equipment. By creating global standards, these organizations enable the possibility of worldwide adoption of UHF RFID. Once ratified, protocols define communication methods approved with the air interface in conjunction with the operating frequency, channel bandwidth, frequency hop rate, etc.

According to RFID management [5] RFID is a transponder technology which is set to play an increasingly important role in the field of logistics alongside existing automatic identification systems such as barcodes. RFID transponders are already in successful use for identifying animals and containers, as part of access control systems, in vehicle immobilizers and in automated production. But the retail and service industries as well as procurement, production and distribution logistics see extended fields of application being opened up by RFID technology, bringing with it greater efficiency in monitoring and controlling supply chains, whether it be in the reduction of stock levels, the optimization of just-in-time processes, the regulation of traffic control systems in ports and airports, the tracking of shipments or in the monitoring of mechanical or climatic influences on goods during shipment. It is assumed that the greatest potential will be in those sectors that have the highest demands on quality and process reliability, such as the pharmaceutical, chemical and automotive industries.

According to A. W. Stcphcn [6], like many technologies, low-cost Radio Frequency Identification (RFID) systems will become pervasive in our daily lives when affixed to everyday consumer items as" smart labels". While yielding great productivity gains, RFID systems may create new threats to the security and privacy of individuals or organizations. This paper presents a brief description of RFID systems and their operation. We describe privacy and security risks and how they apply to the unique setting of low-cost RFID devices. We propose several security mechanisms and suggest areas for future research.

According to J.B. Eom [7] In parallel with the proliferation of radio-frequency identification (RFID) systems, many RFID readers have been increasingly employed. In such an environment, collision among readers becomes a serious problem. Existing anticollision algorithms, depending on the information of neighboring readers, may require constant effort in order to grasp such information. Although it may be given by a server or a coordinator, they may not be suitable in dense and dynamic RFID networks with mobile readers. In this paper, we propose an efficient reader anticollision algorithm using a polling server in dense and dynamic RFID networks with mobile readers. Owing to the assistance of the server, the readers can rapidly decide whether they can work or not without interfering neighbors and can be easily synchronized. Our proposed algorithm is simple and makes readers aware of neighbors to minimize reader collisions. Performance evaluation shows how many readers can operate in a network and indicates that our proposed algorithm is more efficient than distributed color selection, color wave, and hierarchical Q-learning algorithm, particularly in dense and mobile environments.

According to D. M. Konidala [8] Cloned fake RFID tags and malicious RFID readers pose a major threat to RFID-based supply chain management system. Fake tags can be attached to counterfeit products and medicines. Malicious readers can corrupt and snoop on genuine tags. These threats can be alleviated by incorporating a RFID tag-reader mutual authentication scheme. In this paper we propose a simple, cost-effective, light-weight, and practical RFID tag-reader mutual authentication scheme. Our scheme adheres to two ratified standards: EPC global Architecture Framework

specification and EPC global Class 1 Gen 2 UHF RFID Protocol. This scheme utilizes the tag's Access and Kill Passwords and achieves the following three goals: detect cloned fake tags, ward off malicious snooping readers, and in the process, a manufacturer can also implicitly keep track on the whereabouts of its genuine products.

According to P. Perris-Lopez [9]The EPC Class-1 Generation-2 RFID standard provides little security, as has been shown in previous works such as [S. Karthikeyan, M. Nesterenko, RFID security without extensive cryptography, in: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, 2005, pp. 63–67; D.N. Duc, J. Park, H. Lee, K. Kim, Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning, in: The 2006 Symposium on Cryptography and Information Security, 2006; H.Y. Chien, C.H. Chen, Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards, Computer Standards & Interfaces 29 (2007) 254–259; P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard, in: Proceedings of Int'l Conference on RFID Security (RFIDSec)'07, Jul 2007; T.L. Lim, T. Li, Addressing the weakness in a lightweight RFID tag-reader mutual authentication scheme, in Proceedings of the IEEE Int'l Global Telecommunications Conference (GLOBECOM) 2007, Nov 2007, pp. 59–63]. In particular, the security of an RFID tag's access and kill passwords is almost non-existent. Konidala and Kim recently proposed a new mutual authentication scheme [D.M. Konidala, Z. Kim, K. Kim, A simple and cost-effective RFID tag-reader mutual authentication scheme, in: Proceedings of Int'l Conference on RFID Security (RFIDSec)'07, Jul 2007, pp. 141–152] – an improved version of their first attempt [D.M. Konidala, K. Kim, RFID tag-reader mutual authentication scheme utilizing tag's access password, Auto-ID Labs White Paper WP-HARDWARE-033, Jan 2007] – in which a tag's access and kill passwords are used for authentication. In this paper, we show that the new scheme continues to present serious security flaws. The 16 least significant bits of the access password can be obtained with probability 2-2, and the 16 most significant bits with a probability greater than 2-5. Finally, we show how an attacker can recover the entire kill password with probability 2-2.

According to P. Peris Lopez [10] In 2006, EPC global and the International Organization for Standards (ISO) ratified the EPC Class-1 Generation-2 (Gen-2) standard and the ISO 18000 standard respectively. These efforts represented major advancements in the direction of universal standardization for low-cost RFID tags. However, a cause for concern is that security issues do not seem to be properly addressed in these standards. In this paper, we propose a new lightweight RFID tag-reader mutual authentication scheme for use under the EPC global framework. The scheme is based on previous work by Konidala and Kim. We attempt to mitigate the weaknesses observed in the original scheme, and at the same time, consider other possible adversarial threats, as well as constraints on low-cost RFID tags requirements.

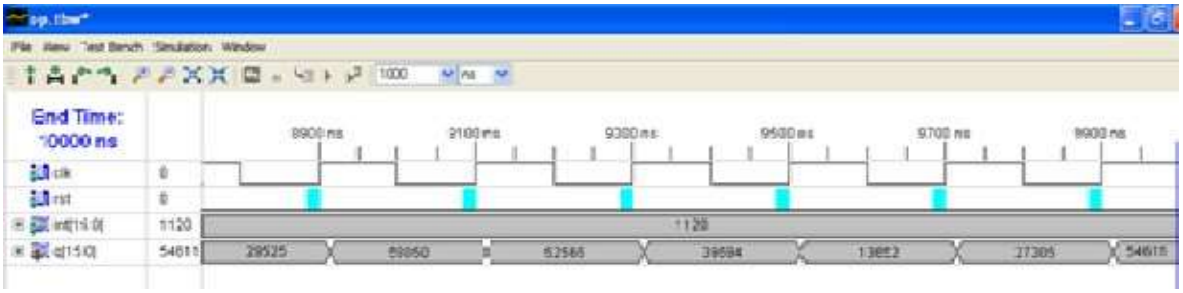
3. OBJECTIVE AND SCOPE

Radio Frequency Identification (RFID) is an automatic identification technology used for remotely retrieving and storing data. Thanks to the non-line- of-sight property of this technology, barcodes are replaced by RFID in many applications. RFID are widely employed and used in various sectors, e.g. warehouse management and logistics, railroad car tracking, product identification, library books check-in/check-out, asset tracking, passport, credit cards. The tag is the basic building block of RFID

systems. Tags contain a unique identification number related to object or person to whom they are attached. The reader is a device that relays information between tags and the back-end server. In secure wireless communication between the tags and the reader prompts many security risks that are similar to security threats of general wireless system. Furthermore, RFID systems have other security and privacy threats that are arising from the accessibility of tags by any reader and compromised tags and readers.

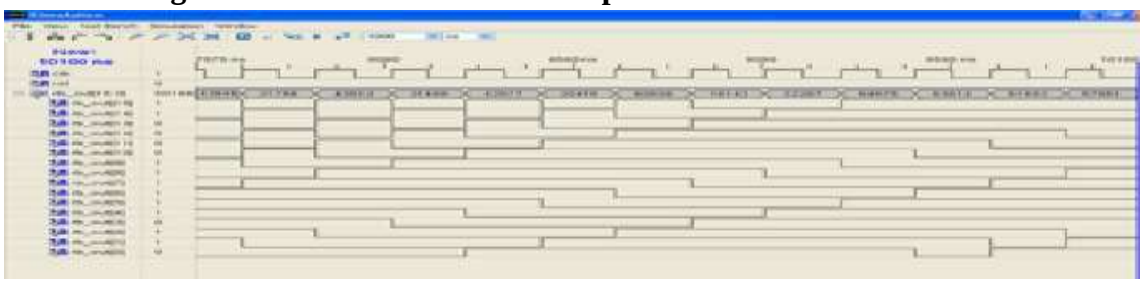
4. RESULTS

Linear feedback shift register

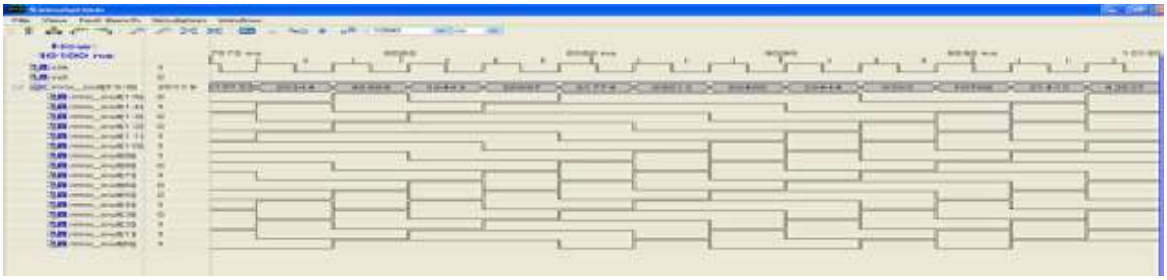


The respective output of Linear Feedback Shift Register (LFSR) is shown in the inputs clk, rst, int are forced to LFSR and the proper output ‘q’ is observed at the output side. Initially value of ‘rst’ is ‘0’, when set to ’1’ the operation will begin till the loop end. The functioning of LFSR is to generate the random numbers

Random Number generates for Manufactures output



Random Number generates for Manufactures



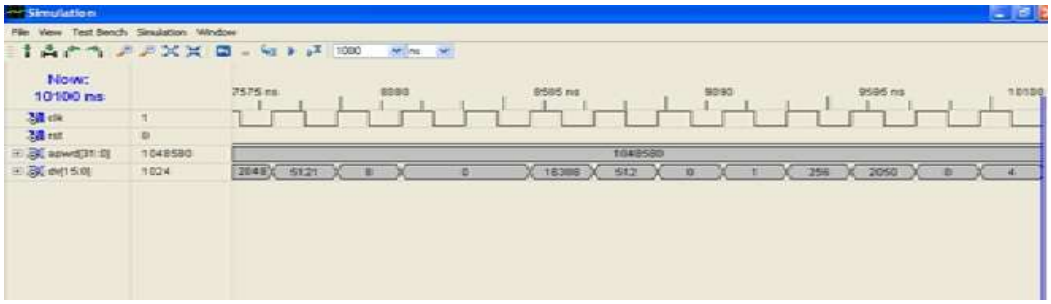
Random Number generates for Tag

The generated LFSR output of random number generation at manufacturer’s side and tag side are shows the inputs are clk, rst, int and the out is ‘q’. Depends on the initial value the random number for tag side or manufacturer’s side will be selected. The generated random number is given as input to the accessing and killing password blocks.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 2, February : 2023

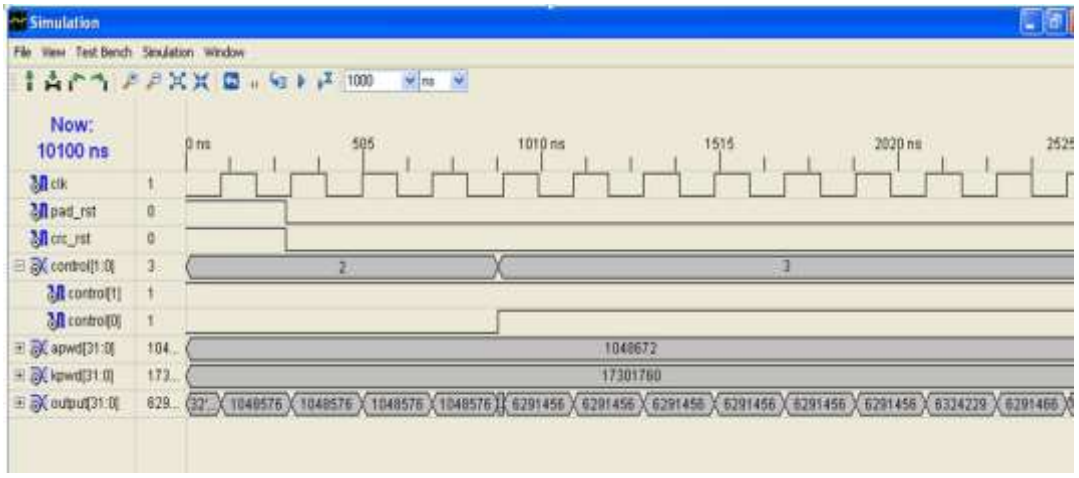
Output of Accessing Password:

Accessing password



The above shows the output snap of Accessing password. In order to generate Accessing password control signal ‘rst’ should be set to ‘0’ and input taken in the above step is ‘1645550’ finally yielded output is ‘2048’. Accessing password is used to access the data in tag authentically. If authentication success tag will send information to reader else mismatch occurs between the tag and the reader.

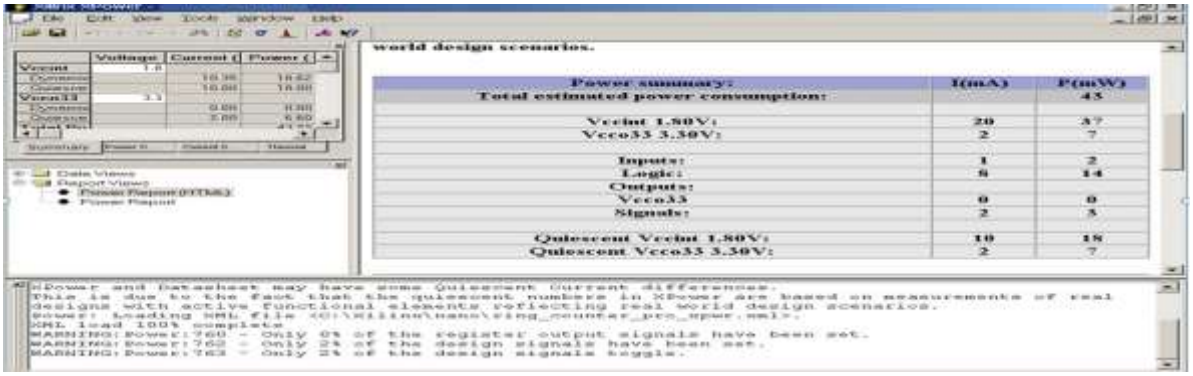
Out waveform for accessing and killing password:



The figure shows the output waveforms of Accessing and Killing passwords. The variables like clk, pad_rst, crc rst, control, apwd, kpwd are forced as inputs and finally the output has cover coded password. The password depends upon the control signals like “00”: accessing password apwdM, ”01”: accessing password apwdL, “10”: cover coded password ccpwdM, “11”: cover coded password ccpwdL. Irrespective of the choice of the user the respective control will be selected. In the snap, the input taken for apwd is 1048672, kpwd is 1730176 and finally cover coded password output is 6291456.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 2, February : 2023

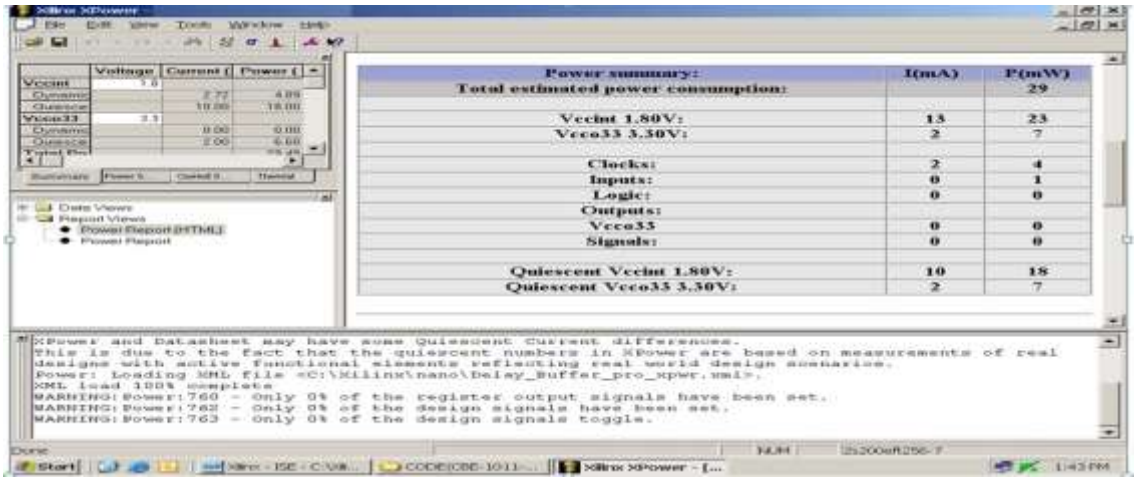
Existed Power report:



Power summary: Total estimated power consumption:	I(mA)	P(mW)
		43
Vccint 1.80V:	20	37
Vcco33 3.30V:	2	7
Inputs:	1	2
Logic:	8	14
Outputs:		
Vcco33	0	0
Signals:	2	5
Quiescent Vccint 1.80V:	10	18
Quiescent Vcco33 3.30V:	2	7

The power report for existed method is shown in Figure. It has the inputs like clk, rst, Apwd, Kpwd gates. For all that power consumed in this base paper is 43 P (mv). The unnecessary clock cycles are applied to all the circuits whenever the global clock is applied. Due to that there is wastage of power, and accessing time will be less in the circuit. This will be improved in proposed method.

Proposed Power report:



Power summary: Total estimated power consumption:	I(mA)	P(mW)
		29
Vccint 1.80V:	13	23
Vcco33 3.30V:	2	7
Clocks:	2	4
Inputs:	0	1
Logic:	0	0
Outputs:		
Vcco33	0	0
Signals:	0	0
Quiescent Vccint 1.80V:	10	18
Quiescent Vcco33 3.30V:	2	7

The power report for proposed method is shown in above figure. It has the inputs like clk, rst, Apwd, Kpwd gates. In the proposed method, the global clock is going to be partition. The power will be reduced by doing active or de-active the selected block. The control of individual blocks is depending on the selection of clock. Due to that the power is consumed and accessing of time is more. In this method the power consumed is 29 P (mv).

Device Utilization Summary:

Selected Device: 3s100etq144-4

Number of Slices: 180 out of 960 18%

Number of Slice Flip Flops: 222 out of 1920 11% Number of 4 input LUTs: 266 out of 1920 13% Number of IOs: 63

Number of bonded IOBs: 63 out of 108 58%

Number of GCLKs: 2 out of 24 8%

Timing Summary:

Speed Grade: -4

Minimum period: 8.741ns (Maximum Frequency : 114.410MHz) Minimum input arrival time before clock :4.845ns Maximum output required time after clock : 4.450n

5.CONCLUSION:

A novel protocol that is both resistant to active attacks and common passive attacks is suggested. The ability to temporarily disable tags without losing any data is another intriguing feature. We sought to learn from prior mistakes when creating our procedure rather than starting from scratch. Three distinct formsof pad-generation function were looked at for the tag-reader mutual authenticationprotocol in the RFID system environment because the EPC Gen2 standard for Class 1 tags only offers a very minimal security level. The proposed method can more effectively address the EPC global C1G2 communication authentication scheme's flaws while using less energy.

References:

1. R. Want, “Enabling ubiquitous sensing with RFID,” Computer, vol. 37, no.4, pp. 84–86, Apr. 2004.
2. T Dimitrio S. Garfinkel and B. Rosenberg, Eds., RFID: Applications, Security, and Privacy. Reading, MA: Addison-Wesley, Jul. 2005.
3. S.Han, H.Lim, and J. Lee, “An efficient localization scheme for a differential-driving mobile robot based on RFID system,” IEEE Trans. Ind. Electron.vol. 53, no. 5, pp. 3362–3369, Dec. 2007.
4. Class 1 Generation2 UHF Air interface Protocol Standard. Available: http://www.epcglobalinc.org/standards
5. Radio Frequency Identification for Item Management, 2nd ed., ISO/IEC18000, Jul. 1, 2008.
6. A. W. Stcphcn, E. S. Sanjay, L. R. Ronald, and W. E. Daniel, “Security and privacy aspects of low-cost radio frequency identification systems, “Security Pervasive Compute., vol. 2802, pp. 201–212, 2004.
7. J.B. Eom, B.Yim and T.J. Lee, “An efficient reader anti-collision algorithm in dense RFID networks with mobile RFID read,” IEEE Trans.Ind. Electron vol. 56, no. 7, pp. 2326–2336, Jul. 2009.
8. D. M. Konidala, Z. Kim, and K. Kim, “A simple and cost effective RFID tag–reader mutual authentication scheme,” in Proc. Int. Conf. RFID Sec, Jul. 2007, pp.141–152.Perris-Lopez, T. Li, L. Lim, J. C. Hernandez-Castro, and J. M. Estevez- Tapiador, “Vulnerability analysis of a mutual authentication scheme underthe EPC class-1 generation-2 standard,” in Proc. RFID Sec, Jul. 2008, pp. 52–63.
10. P.PerisLopez, T.-L. Lim, and T. Li, “Providing stronger authentication at alow cost to RFID tags operating under the EPC global frame work,” in Proc. IEEE/IFIP Int. Conf. EUC, Dec. 17–20, 2008, vol. 2,pp. 159–