Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 11 (2013) 778 – 784

Procedia Technology

The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013)

Computational Cost Analysis on Securing RFID Protocols Conforming to EPC Class-1 Generation-2 Standard

Azam Zavvari[a,*], Masoud Shakiba[a,b], Mohammad Tariqul Islam[c], Elankovan Sundararajan[b], Mandeep Jit Singh[a,c]

[a]*Department of Electrical Electronic and Systems Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia*

[b]*Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia*

[c]*Institute of Space Science (ANGKASA), Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia*

Abstract

A Radio Frequency Identification (RFID) system is a contactless automatic identification system that uses small and low-cost tags. RFID systems communicate with the tags attached to the objects using radio frequency waves. The major problem with RFID systems is the security problem because the communication between RFID components is wireless. In this paper, we comprehensively discuss the computational cost and vulnerabilities of the security Protocols on RFID systems. We presented an improvement mutual authentication protocol which can prevent the security problems and easy to implement in low-cost passive tags, with low computational cost. The proposed protocol is compatible with the international standard EPC Class-1 Generation-2 standard (ISO 18000-6).

Selection and peer-review under responsibility of the Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia.

Keywords : RFID; EPC Class-1 Generation-2 Standard; ISO 18000-6; Computational Cost; Security and Privacy.

1. Introduction

Due to low-cost, convenience, and efficiency of Radio Frequency Identification (RFID) systems, uses of this technology have become an inseparable part in our daily lives. RFID systems consist of three main components: tags, reader, and server (database) as shown in Fig. 1. Tags are attached to the objects to identify them as unique

* Corresponding author. Tel.: +6-014-222-0450.
E-mail address: azam.zavvari@gmail.com

Selection and peer-review under responsibility of the Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia.
doi:10.1016/j.protcy.2013.12.258

objects. The tags are containing a microchip and antenna. The tags send and receive data from the reader, which is connected to a server [1].

Fig. 1.Components of RFID

RFID tags are generally categorized into passive tag, semi-passive tag and active tag based on their source. The inexpensive and smallest tags are passive tags which it is more popular than other types. The passive tag powered by an electronic signal emitted by RFID reader. Semi-passive depends on battery to run its own microchip and signals are powered by the reader. Active tags are powered by on-board battery. The active tags communicate in a wide range because of on-board battery. Active and semi-Passive tags are expensive and contain more hardware than passive tags [2, 3].

RFID systems have various applications, such as national identification; collecting tolls without stopping; wireless traffic management, automating vehicle parking; automated toll collection, animal identification; asset management; airline passenger baggage; animal identification; hotel and resorts; tracking library books; warehouse management; smart house; security of items which should not leave the area and a high usage of RFID systems are in healthcare and medicine [4-6].

The usage of RFID systems is increasing rapidly with products supplied by multi-vendors, requiring a worldwide set of Electronic Product Code (EPC) standards. Fortunately, the EPCglobal organization has started to develop these standards. Despite this standard initiative, the security and privacy issues with RFID systems are not well addressed yet. RFID technology poses several security and privacy threats that could harm its global proliferation and usage. International standards have many benefits, such as supporting the proliferation of the RFID systems and decreasing the global costs [7].

All ISO standards are required to be available around the world, so users of ISO RFID standards will not be worried any more if their systems comply with the different ISO regulations on frequencies and power output for each country where business is made. ISO has been working on RFID applications in several areas. The standards are divided into four main groups, which are ISO standards for proximity card (ISO 14443) and vicinity cards (ISO 15693), RFID air interface (ISO 18000), animal identification (ISO 11784, ISO 11785) and ISO supply chain standards (ISO 17358, ISO 17363-17367, ISO 17374.2) [8]. Table 1 show different parts of RFID air interface standard and deals with a different aspect of this standard and explain how these ISO 18000s work.

Table 1. Different aspect of RFID air interface.

ISO	Parts
ISO 18000-1	Generic Parameters for Air Interface Communication for Globally Accepted Frequencies.
ISO 18000-2	Parameters for Air Interface Communication below 135 KHz (Standard for Low Frequency)
ISO 18000-3	Parameters for Air Interface Communication at 13.56 MHz (Standard for High Frequency, R\W capability)
ISO 18000-4	Parameters for Air Interface Communications at 2.45 GHz (Standard for Microwave Frequency, R\W capability)
ISO 18000-5	Parameters for Air Interface Communication at 5.8 GHz
ISO 18000-6	Parameters for Air Interface Communication at 860 – 930 MHz (Standard for UHF Frequency, R\W capability, also it known as EPC Class-1Generation-2)
ISO 18000-7	Parameters for Air Interface Communication at 433.92 MHz