Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 336 – 341

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Multilevel Secure RFID Based Object Tracking System

Ajinkya C Bapat[a*], Sonali U Nimbhorkar[b]

[a]ME Student, Department of Computer Science & Engineering ,G.H.Raisoni College of Engineering, Nagpur,440016,India
[b]Department of Computer Science & Engineering, G.H.Raisoni College of Engineering, Nagpur,440016,India

Abstract

Security is an important issue in our everyday life. System based on different wireless protocol standards is vulnerable to security threats. This Paper is giving glance on security issues arises in object tracking system; and to deal with that, provide comparative analysis between various cryptographic techniques for selecting best one among all. The use of 128 bit PRNG and XOR protocol across RFID system and applying Binary ECC while sending data via GSM communication will surely boost up safety measures of object tracking system as depicted in this paper.

Keywords: RFID;GSM;XOR &128bit PRNG; Binary ECC

1. Introduction

Radio Frequency Identification (RFID) technology can be used across variety of application. The use of RFID tracking can be effectively implemented in object tracking, tracking of material and items in mall or large shopping complex, vehicle tracking, farming etc. Today RFID is used widely across world; as per survey published in 2013, the use of RFID technology for various application is increase at the rate of 15 percent per annul year. It is possible that we may be dependent on RFID technology for many reason just like we are dependent on use of cell phones, E-mail , Computers, internet etc[1].

RFID system has two important parts as RFID card and RFID Reader. Each card has unique identification number stored inside it. RFID Reader traces valid card if it found math match of unique number of tag with the data stored in it. RFID tag usually consists of antenna for transmission and reception of Radio Frequency (RF) signal[3].One of the highlighting point of RFID Technology is ability of RFID Reader to trace out the particular tag

*Corresponding author. Tel.: +91-7276829506;
E-mail address: ajinkyabapat1@gmail.com

doi:10.1016/j.procs.2016.02.068

among group of cards and while tracing it READER and TAG must have Line of Sight communication between Them[4].Various security issues are present in RFID tracking system like Reply attack, Denial of services (DoS),Card Reader Anonymity, card –reader location privacy etc. A lots of efforts has been taken till date to sort out all the security related issues; but The use of 128 PRNG and XOR effectively deals with all the security threats present with less requirement of storage for its implementation as proposed in[1, 18].

The position of object traced by RFID system is located by using Global Positioning system (GPS) and its co-ordinate can be send using Global System for mobile communication (GSM) module to the Authorized person or care taker of that object. GSM communication also vulnerable to security threats as it performs its operation using Air interface. Use of mobile phones has increases rapidly day by day .Wireless protocol and cellular technology uses air interface for its operation and it is more vulnerable to security threats than wired technology. It may possible that anyone at receiving side whether it is authorized or unauthorized may access the calls and text messages. One can easily imagined how unsafe it is if someone access your phone call, messages, bank details etc[2, 4].The location of object positioned by GPS may be access by unauthorized person during its transmission via GSM. For this it is necessary to use effective security protocol while using GSM communication[3].

It is essential to provide security provision to object tracking system, so that object can be tracked without any attack and its location can be sent to authorized person through air interface confidentially. The use of security protocol at two ends will definitely solve the security issues while tacking the object[1, 11,12,13,18].

The aim of this paper is to analyze the use of 128 bit PRNG and XOR encryption technique and Binary ECC across RFID and GSM module respectively. This paper will also highlight the fact that, how effective this techniques in comparison to other techniques for enhancing the overall security of object tracking system. The rest of the paper is organized as follows, in Section 2 the related work for applying security protocol in object tracking system is given, Section 3 analyze the effectiveness of Binary ECC over Prime Field ECC , Proposed system is describe in section 4 and the conclusion is drawn in Section 5.

2. Related Work

In object tracking system RFID Reader and RFID tags are important parts. Passive RFID tag has limited storage space to apply security protocol, Because of this while selecting security protocol it is necessary to think about storage space of RFID Tag[9]. Many of the security approaches applying across RFID system do not fulfil the storage requirement because it uses Hash function which require Large storage space in the range of 8k to 10k[1,4]. Passive RFID Tag is able to provide limited storage space up to 3k to implement security provision[1, 4,8,10]. Such limited storage space is also insufficient to apply security aspect using simple symmetric encryption techniques like RSA[1,13].Although cheaper cryptographic alternatives such as elliptic curve cryptography (ECC) exist, the realistic execution of ECC is still an area to explore .Execution of ECC would require around 8.2 and 15K corresponding gates[1, 12]. Symmetric encryption techniques like Advanced Encryption standard (AES) require approximately 3.4k gates[1, 11]. The protocol used 128 bit PRNG which is proved to be secure and requires less than 2 K gates[1].

2.1. Security offered by 128 bit PRNG and XOR

- The use of 128 bit PRNG and XOR Protocol will combat against following security threats as mentioned in[1,11,12,13,18].
- Tag/Reader Anonymity : The protocol protects against information leakage which cause the leakage of information of original user of reader. Because of this protocol it is difficult to make a replica of the authorized or valid reader or card.
- Tag/Reader Location Privacy : This protocol avoid the expose of tag/reader location and thereby hides the information about its user.
- Forward Secrecy : The protocol ensures that on compromise of the internal secrets of the tag, its previous communications cannot be traced by the attacker. This requires that previous messages are not dependent on current resident data on the tag.
- Replay Attacks : The protocol resists compromise by an attacker through the replay of messages that have been collected by an attacker during previous protocol sequences. This requires that protocol messages in each round of the protocol are unique.