Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.6, No.9, 2015
www.iiste.org

A Brief Survey of RFID Devices and Its Security Protocols

Rakesh Chandraul Rajat Paliwal Anurag Jain
Department, Computer Science and Engineering
Radharaman Institute of Technology and Science Bhopal Madhya Pradesh INDIA

Abstract
Security plays a very important role during the transmission of information in RFID devices. RFID are the wireless devices that contain a tag and a reader. While there are many authentication protocols put into operation for the security of data starting the tag to the reader. The main purpose of this brief survey is to provide the information of the most related privacy and security protection protocols which applied to Radio Frequency Identification operation. The aim of this paper is to choose to most relevant protocols for RFID devices security.
Keywords: RFID, HECC, RSA, AES, ECC.

I. INTRODUCTION

A Radio Frequency Identification (RFID) system consists of tags (or transponders) that store up data and transfer the data to readers (or interrogators) over a wireless network. In practical RFID method the readers are networked to a wider activity computer system. The major function of an RFID method is to facilitate tagged items or persons to automatically position their identity to other systems wirelessly [1].

RFID system is the most up-to-date technology that the stage an important role for object identification as everywhere infrastructure. RFID has several Applications in right to use control, built-up computerization, maintenance, supply series management, Parking, garage, management, automatic fee, tracking, and record control. RFID tag is a little radio chip that includes a simple silicon microchip bond to a small smooth aerial and accumulates on a substrate. The complete device can then be summarizing in dissimilar materials (such as plastic) reliant upon its planned usage. The tag can be emotionally mixed up to an object, usually an item, box, or pallet, and understand writing remotely to establish its characteristics, location, or state. In favour of an active tag nearby will as well be a battery. Reader or Interrogator: send and receives RF data to and on or after the tag via aerial. A reader may have a number of antennas that are dependable for sending and receiving radio effect [2].

RFID offer some advantages over barcodes: data are recognize automatically, line of sight not mandatory, and through non conducting materials at high speed and far distance. The reader can understand the contents of the tags by distribution RF signals via antennas. The tags data handle by the readers are then accepted to a host computer, which may sprint middleware (API). Middleware recommend processing modules or services to decrease load and network traffic contained by the back-end systems.

As shown in figure 1.1 we describe the basis operation of RFID Devices. The object to be gone behind is attached among a RFID tag or transponder[9]. The reader, set aside at some position like opening or door frame from side to side which objects to be tracked pass, release radio signals. While the object surrounds RFID tag approach within the variety of radio signals released by the reader, the tag is turn on and it
starts sending the information store up in it in the outline of radio signals. The reader confine the radio signals, translate it to a byte stream, and send the information for further bountiful out to the host method connected to it.

RFID systems are exposed to a broad range of spiteful attacks choice from passive overhear something to active interference. Nothing like in wired networks, someplace computing systems naturally have equally centralized and host-based barricade (e.g. firewalls), attacks moving RFID networks can goal decentralized parts of the method infrastructure, as RFID readers and RFID tags function in an inherently not fixed and potentially deafening environment.

RFID tags may cause a considerable security and privacy possibility to organizations and individuals via them. Since a typical tag response its ID to any reader and the answer back ID is always the same, an attacker can simply hack the arrangement by reading away the data of a tag and duplicating it to fake tags. Vulnerable tags may contain vulnerabilities to nose round, position privacy, spoofing, or denial of service (DOS). Unauthorized booklover may compromise privacy by right of entry tags without enough access control. Even once the content of the tags is sheltered, those may be tracked through conventional tag responses.

RFID Frequencies Bands and its characteristics:

RFID methods are generally distinguished to three frequency variety Based on the type of province or application targeted Low, in-between and high. The following table 1.2 review these three frequency ranges, the length of with the typical system behavior and examples of major part of application [1].

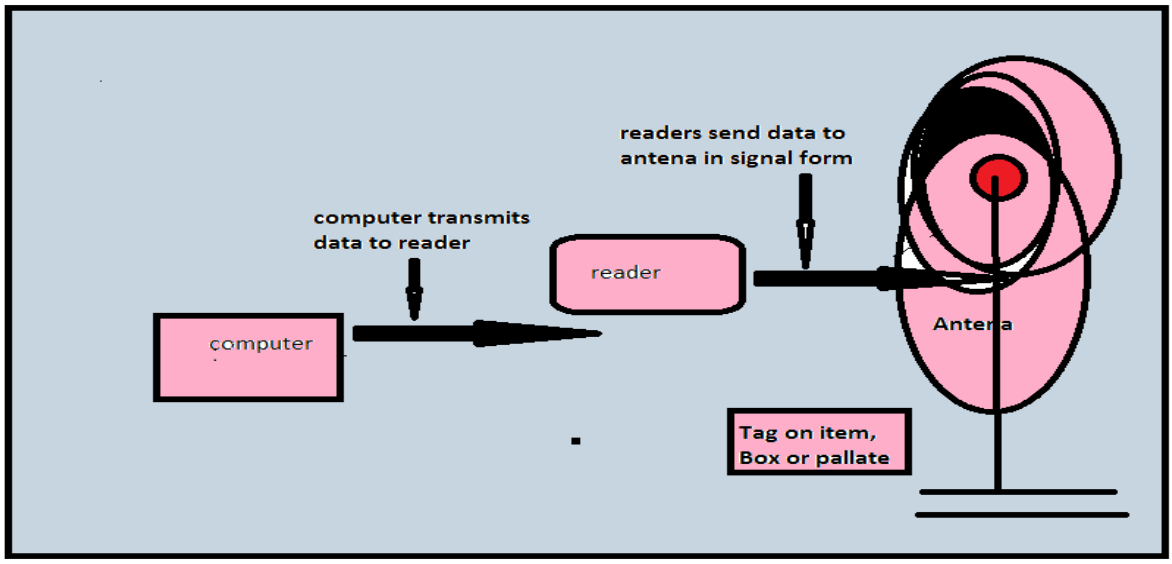

Figure 1.1: Basic Operation of RFID

Table 1.1: RFID Frequencies

Frequency Ban	Characteristics	Typical Applications
Low 100-500 KHz	Short to medium read range, inexpensive, low reading speed	Access control, Animal identification
Intermediate 10-15 MHz	Short to medium read range, potentially , medium reading speed	Access controls, Smart cards
High 850-950 MHz 2.4-5.8 GHz	Long read range, high reading speed	Railroad car monitoring, Toll collection systems

II. Organization of the paper

The plan of the paper is organized as follows: In Section I Introduction, In Section II Organization of the paper, In Section III review related work and discuss our contributions, In section IV discuss problems statements of RFID devices, In section V forms security protocols for RFID devices, In section VI describes hyper elliptic curve cryptography, In Section VII we outline the research scope efforts related to RFID, and then In Section VIII conclusion. We bring to a close with some references in Section IX.

III. Related Works

In 2010 Gyozo Godor, Norbert Giczi, Sandor Imre Considering the limitation of the length of the contribution we can only introduce to ECC based authentication protocols briefly. The EC Based Mutual Authentication Protocol The authors suggest the use of curves[3] while implementing the protocol, This protocol is highly based on the assumption, that the Montgomery-ladder implementation calculates using only x coordinates. The input of the Montgomery-algorithm is not the complete point, but only its affine x coordinate, while its output is the emerged point's projective (X, Z) coordinate pair. This way, the y coordinate of the curvepoints is practically unneeded during the runtime of the protocol, which lowers the size of the messages [3].

In 2012 Matthew Butler, Peter J. Hawrylak and John Hale planned Dynamic Risk Assessment Access Control (DRAAC) protocol for imposition detection, it reduces contact privileges in RFID access control system. by using This method allows one to secure the most sensitive areas of a facility while minimizing the range to which legitimate users are restricted. [4].

In 2012 A. Anny Leema1, Dr.Hemalatha.M [5] planned a technique to improve the quality of data. This approach is a mixture approach of middleware and deferred because it is not always potential to remove all anomalies and redundancies in middleware. It performs the cleaning in an effective manner.

In 2012 Tuan Anh Pham,Mohammad S. Hasan and Hongnian YuIn suggest the mutual authentication protocol based on the challenge response model. The Advanced Encryption Standard (AES) is used as a cryptographic archaic to secure the data it is a mutual authentication protocol which utilizes AES-128 as a primitive to encrypt the messages transmitted on the channel. With that cipher block, the protocol can protect

against many types of attacks such as information leakage, tag tracking etc [6].

IV. Problem Statement

Elliptic Curve Cryptography Based Mutual Authentication Protocol is a very good security protocol. and well security provides. ECC uses key is 112, 160 and 192bits. But here we use another new protocol this is a HECC algorithms. HECC key size is less then comprasion to ecc. This protocol gets the well result in comparison to ECC protocol, in terms of performance and security in same security level[3][12].

AES algorithms used to provide the security of RFID devices. But AES algorithms problem is use to permutations for each cycle, so AES algorithms is time consuming and increase the time complexity of our system [6][12].

RSA algorithms is a very secure algorithms but this algorithms use large prime numbers and RSA mathematical calculation is time consuming modular exponential, so increase the storage cost and computational time of the our system [11][3].

V. Security Protocols for RFID Devices

AES Algorithms

AES is an Advanced Encryption Standard algorithms and well encryption/decryption cryptography system. This algorithm used to be securing the data from hackers. AES is based on substitution permutation network, AES algorithms use the block size is 128 bits, and use key size is 128, 192 or 256 bits. This algorithm is use minimum key size is 128 bits and maximum is 256 bits. The

number of cycles of repetition is as follows: This algorithms use to secure the RFID devices and easy to implement. And more study about the RFID devices privacy and security by the AES algorithms [6]. So this is very good algorithms but this algorithms drawbacks is a large key size, more permutation and more storage cost.

ECC Algorithms

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to generate faster, smaller, and other efficient cryptographic keys[9]. ECC generates keys through the properties of the elliptic curve equation instead of the established method of generation as the product of very large prime numbers. The technology can be used in concurrence with most public key encryption methods, such as RSA, and Diffie-Hellman[10].

VI. Hyper elliptic Curves Cryptography

This algorithms use to we secure the RFID Devices because this algorithms is use global variables. The security of hyper elliptic Curve Cryptosystem depends on the discrete logarithm problem. This problem helps to avoid the eavesdropper from breaking of keys even both Q and P values are famous publicly. Different types of arc have to study to recognize about public key (Q), set point (P) and Hyper elliptic Curve Discrete Logarithmic problem (HECDLP) [7].

Hyper elliptic curve E of genus g>=1 over fixed filed F is the set of solution (x,y) ϵ F*F to the equation

E: $y^2 + h(x)\, y = f(x)$ (1)

Where h(x) is a polynomial of degree g and h(x) ϵ F(x), f(x) is a monic polynomial of measure 2g+1 and h(x) ϵ F(x). The curve E is said to be non-singular curve, if there are no pairs (x, y) ϵ F*F. The polynomial f(x) and h(x) are chosen such that it has to satisfy the following equations

$2y + h(x) = 0$ (2)

$h'(x)\, y - f'(x) = 0$ (3)

Types of genus curve

Genus curve decide the processing time of the hyper elliptic Curve Cryptosystem such as key generation, encryption and decryption process. Value of g decided the polynomial of curve E like g = 2, 3, 4. Polynomial chosen for genus 2, 3, 4, 5 and 6 over prime field Fp is given below

Genus g=2

$Y^2 = x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$ (4)

Genus g=3

$Y^2 = x^7+a_6x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$ (5)

Genus g=4

$Y^2=x^9+a_8x^8+a_7x^7+a_6x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+ a_1+a_0$ (6)

Genus g=5

$Y^2=x^{11}+a_9x^9+a_8x^8+a_7x^7+a_6x^6+a_5x^5+a_4x^4+a_3x^3+ a_2x^2+a_1x+a_0$ (7)

Genus g=6

$Y^2=x^{11}+a_9x^9+a_8x^8+a_7x^7+a_6x^6+a_5x^5+a_4x^4+a_3x^3+ a_2x^2+a_1x+a_0$ (8)

Jacobian of Hyper elliptic Curve The Jacobian of curve E defined over finite field F is represented by JE(F) [7].

Each elements of the Jacobian can be represented uniquely by a divisor D as shown Eq. (4) and Eq. (5).

$J_E(F) = D_0/p$ (9)

$D = \sum m_i p_i$ (10)

Where D is called as reduced divisor mi Number of points, Pi Points on the Curve E The reduced divisor D is represented using Mumford representation which forms the group law in Jacobian of a Hyper elliptic Curve [7]. HECC consist of three procedures such as key generation, encryption and decryption. These processes involved in divisor generation as shown in Equation (10) by choosing proper polynomial of genus curve 2, 3, 4, 5 and 6 as shown in Equation (4), (5), (6), (7) and (8). ElGamal method is used to design Hyper elliptic Curve Cryptosystem process, known as HECElGamal algorithm as shown below :

Key generation

Input: The public factor are hyper elliptic curve C, prime p and divisor D.

Output: The public key P_A and private key a_A.

method:

Private Key: $K_A \in RN$; Random prime number K_A is chosen in order of N.

Public key: $P_A \leftarrow K_A.D$;

P_A is represented as pair of polynomial [(u(x), v(x))] and D is Divisor

Key pair: $[(K_A, P_A)]$

Encryption algorithm

The plaintext 'm' is converted into ASCII value and these values are represented as Sequence of points (u_x, v_y). The encoded message is referred as Em. The following steps are

Followed to encrypt the encoded message Em of user A and send it to user B.

Private Key: $K_A \in RN$; Random prime number K_A is chosen in order of N.

Public key: $P_A \leftarrow K_A.D$;

P_A is represented as pair of polynomial [(u(x), v(x))] and D is Divisor

Agreed key: $Q_A \leftarrow K_A.P_B$; PB is represented as receiver's public key.

Cipher text: $C_m \leftarrow \{Q_A, E_m + P_A\}$; C_m is represented as [(u(x), v(x))].

Decryption algorithm

To decrypt the cipher text Cm, user B extracts the first coordinate 'QA' from the cipher text next multiply with its private key (a_B) and take away the result from the second coordinate. This can be printed as follows:

$E_m + k P_B - a_B (Q_A) = E$

$= E_m + k P_B - k (a_B D)$

$= m + k P_B - a_B (k D)$

$= E_m + k P_B - k P_B = E_m$

VII. Research Scope

Various researches in RFID fields and the study in research survey of RFID refer to [1], [8]:

Asset Tracking: fixed or in-motion assets path or locating, similar to a healthcare ability, wheelchairs or laptops in a company and servers in a data heart, was not so simple task.

People Tracking: People tracking scheme are old just as asset tracking scheme. Hospitals and jails are nearly everyone general tracking vital places.

Document tracking: This is mainly common problem. Availability of great amount of data and documents carry lots of problem in file management system.

Library System: RFID tools uses for reading these barcodes different the self-barcode reader RFID motorized barcode reader can understand multiple items simultaneously. This ease queues and raises the number of clients using self-check, which in roll will ease the staff necessary at the movement desks.

VIII. Conclusion

In this paper we have briefly analysed the most relevant privacy and security protocols for RFID technologies. The aim of this survey is to secure the RFID Devices and select the protocols. And selecting protocols have less storage cost and computational time as well as it can also provides security from various types of attacks such as mutual authentication, forward secrecy, replay attacks and also the number of bits generated for the session key. The efficiency of the choosing algorithm is very high because it is not concerned in any types of time consuming modular exponential work out. Although the list of analysed protocols is far from complete, we believe that all the selected protocols are relevant and they provide the reader with a proper overview of the security and privacy issues related to the RFID technology.

IX. References

[1] Charles Mutigwe and Farhad Aghdasi, "Research Trends in RFID Technology", pp. 1-10.
[2] Tuan Anh Pham, Mohammad S. Hasan and HongnianYu "A RFID mutual authentication protocol based on AES Algorithm", IEEE, pp. 997-999, 2012.
[3] Gyozo Godor, Norbert Giczi, Sandor Imre, "Elliptic Curve Cryptography Based Mutual Authentication Protocol for Low Computational Capacity RFID Systems - Performance Analysis by Simulations", IEEE, pp 650-657, 2010.
[4] Matthew Butler, Peter J. Hawrylak and John Hale, "Graceful Privilege Reduction in RFID Security" , 2011 CSIIRW, Article No. 47, pp.47+12, Oct 2012..
[5] A.Anny Leema, Dr.Hemalatha.M "A New Deferred cleansing technique for Effective Warehousing of RFID", (CCSEIT"12) Second International Conference on Computational Science, Engineering and Information Technology, pp. 626-631, 2012.
[6] Tuan Anh Pham, Mohammad S. Hasan and Hongnian Yu "A RFID mutual authentication protocol based on AES Algorithm", IEEE, , pp. 997-999, 2012.
[7] P. Vijayakumar1, V. Vijayalakshmi2 and G. Zayaraz, "Comparative Study of Hyperelliptic Curve Cryptosystem over Prime Field and Its Survey", International Journal of Hybrid Information Technology, vol. 7, pp. 137-146, (2014).
[8] Charles Mutigwe and Farhad Aghdasi, "Research Trends in RFID Technology", School of Electrical and Computer Systems Engineering Central University of Technology, Free State, South Africa, pp 1-15.
[9] Ya-li Liu, "A Lightweight RFID Authentication Protocol based on Elliptic Curve Cryptography" , JOURNAL OF COMPUTERS, VOL. 8, NO. 11, NOVEMBER 2013.
[10] Mustapha Benssalah , Mustapha Djeddou , Karim Drouiche , "Efficient ECC Implementation Architecture Suitable for RFID Technology" , IEEE, pp , 2012.
[11] Jonathan Sangoro, DR. Michael Kimwele, "Enhancement of Security in RFID using RSA Algorithm", IISTE, Vol 5, pp. 65-69, 2014.
[12] Marietta, Georgia, Kaige Kang, Yue Shi, "Research on Encryption Model Based on AES and ECC in RFID" IEEE, PP 9-13, 2013.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar