Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.6, No.12, 2015

Efficient Security of RFID Devices using HECC Algorithms and Performance Analysis by Simulation

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

Abstract
RFID technology is able to be established in the most meadow of our daily life, e.g. personal identification, supply-chain management, access control etc. Radio Frequency Identification (RFID) is the devices which contain tag and reader which communicated wireless through radio waves. Hence security of data is most important so that any other unauthorized person cannot be access it. even though there are various method implemented for the protection of data during wireless communication which provides security from different attacks such as DoS, replay, mutual authentication etc. but these techniques are consume large amount of storage space and computation time Here in this paper we proposed a Hyper Elliptic Curve Cryptography (HECC) which provides security from different attacks. Our comprehensive result shows that proposed method is better in conditions of storage space and computation time.
Keywords: RFID, HECC, Privacy and Security, Tag, Reader.

I INTRODUCTION

An RFID structure consists of tags with the intention of store up data and transmits the data to readers more than a wireless network. In realistic RFID technique the readers are set of connections to a wider movement computer system.[4] The major function of an RFID technique is to make easy tagged items or people to automatically site their individuality to other structure wirelessly [1].

RFID classification is the most the latest technology that the point an important role for object detection as everywhere infrastructure. RFID has more than a few Applications in correctly to use control, built-up mechanization, maintenance, supply progression management, Parking, garage, management, mechanical fee, tracking, and confirmation control. RFID tag is a diminutive radio chip that includes an effortless silicon microchip friendship to a small smooth above ground and accumulates on a substrate. The entire device can then be summarizing in disparate materials (such as plastic) conditional upon its planned usage.[6] The tag card can be emotionally varied up to an item, usually a piece, container, or pallet, and understand writing slightly to establish its characteristics, position, or shape. In favors of an active tag nearby will as fit is a battery. Reader or Interrogator: pitch and obtain RF data to and on or after the tag via above ground. A reader may comprise a number of antennas that are reliable for transfer and in receipt of telephone system effect [9].

RFID offer various advantages over barcodes: data are being familiar with automatically, row of sight not mandatory and from side to side non conducting equipment at high rapidity and remote distance. The reader can comprehend the stuffing of the tags by giving out RF signals by way of antennas. The tags data touches by the readers are then accepted to a congregation computer, which may tear middleware (API). Middleware propose processing component or services to decline pack and network interchange restricted by the back-end arrangement [16].

We describe the basis process of RFID Devices. The object to be disappeared behind is attached among a RFID tag or transponder [9]. The reader position aside at some location like opening or entry frame from side to side which objects to be tracked overhaul, let loose radio signals. While the article surrounds RFID tag approach contained by the variety of radio indicate released by the reader, the tag is turn on and it starts sending the in sequence store up in it in the delineate of radio signals. The reader impound the radio signals, transform it to a byte flow, and send the information for auxiliary bountiful out to the congregation technique related to it[14].

RFID systems are uncovered to a extensive range of hurtful attacks choice from passive eavesdrop something to active interference. Nothing similar to in restless networks, wherever computing systems as expected have equally federal and host-based hurdle (e.g. firewalls), attacks affecting RFID networks can goal decentralized parts of the procedure transportation, because RFID readers along with RFID tags role in an inherently not fixed and potentially deafening situation[10].

RFID tags may origin a substantial security and privacy option to group and individuals by way of them. given that a typical tag response its ID to a few reader and the counter back ID is always the same, an attacker can simply lacerate the arrangement by reading away the data of a tag and duplicating it to counterfeit tags. Vulnerable tags may contain vulnerabilities to nudge round, position privacy, spoofing, or denial of examine (DOS). Unauthorized booklover may compromise privacy by right of way in tags without enough access control. Even some time past the content of the tags be sheltered individuals may be tracked through conventional tag comeback. RFID Frequencies are crowd and its exceptionality [14].

RFID techniques are generally distinguished to four frequency variety Based on the type of province or application targeted Low, high, ultra high and microwave, the length of with the typical system behavior and examples of major part of application [1].

II. ORGANIZATION OF THE PAPER

The arrangement of the paper is planned as follows: In Section I Introduction, In Section II association of the paper, In Section III review related work and converse our contributions, In section IV discuss implementation of the protocol, In section V system model in omnetpp, In section VI security and privacy analysis, In Section VII result analysis, In section VIII conclusion and then In Section IX future enhancement. We bring to a close with some references in Section X.

III. RELATED WORKS

In 2010 Gyozo Godor, Norbert Giczi, Sandor Imre creation an allowance for the limitation of the distance end to end of the giving we can only initiate to ECC based verification protocols briefly. The EC support Mutual Authentication procedure the authors suggest the create use of curves [3] though implementing the procedure; this set of rules is highly bottom on the assumption, that the Montgomery hierarchy implementation calculates by means of just x coordinates. The input of the Montgomery procedure is not the whole point, but only their affine as manage, while its productivity is the emerged point's projective (X, Z) synchronize pair. This way, the y synchronize of the curve points is basically unneeded throughout the runtime of the procedure, which worse the size of the messages [12].

In 2012 Matthew, Peter J. Hawylak and John planned active Risk Assessment way in Control (DRAAC) procedure for imposition finding, it trim down contact privileges in RFID way in control system. By means of this technique allows one to protect the most receptive areas of a competence while decrease the ranges to which legal users are constrained [6].

In 2012 A. Anny Leema1, Hemalatha [13] intended a procedure to recover the quality of data. This come within reach of is a combination come near of middleware and delayed because that is not always latent to remove all variance and redundancies in middleware. It performs the cleanout in a valuable manner.

In 2012 Tuan Anhh Pham, Mohammaad S. Hassan and Hongnia advise the mutual confirmation procedure based on the brave reply model. The Advanced Encryption Standard (AES) is shabby as a cryptographic antiquated to safe and sound the facts it is a common confirmation protocol which make the most of AES-128 as a primal to encrypt the letters transmitted on the waterway. With that symbols block, the procedure can protect next to many types of do violence to such as in a row leakage, tag tracking etc [11].

IV IMPLEMENTATION OF THE PROTOCOL

A hyper elliptic curve 'C' of type g defined larger than a country side Fq of quality p is specified by an equation of the figure

$y2+ h(x)\ y = f(x)$ over Zp

Where h(x) and f(x) are function of x by way of coefficients in Fq by way of deg h(x) <=g and deg f(x) =2g+1. And h(x) and f(x) is a function of x. here g is a generator and p is a prime number. Calculations of the alpha by the help of slope equation hear we firstly select two point g. suppose g is a generator and it a coordinate type point is (x, y) Then we calculate 2g.

Means $2g = g + g$

Here points are same, so we solve λ

$\lambda = (3*x^2+1)\ (2*y)^{-1} \bmod p$

If points are different then, suppose a point is $(x_1,y1)$ and (x_2,y_2) then calculation of λ is

$\lambda = (y_2-y_1)\ (x_2-x_1)^{-1} \bmod p$ Then after we solve next invention point this is (x_r, y_r)

So $x_r = \lambda^2-x_1-x_2$ and

$y_r = \lambda(x_1-x_3)-y_1$

Is next point is (x_r, y_r) and follow the same process and we generate many points. Then our system select randomly. Then after we have a set of points this is called generator. i.e. g, 2g, 3g, 4g…….so on.

Hence we already know (x, y) is indeed primitive element. We derive the following Dynamic primitives:

- ✓ Setup
- ✓ Key gen
- ✓ Encryption
- ✓ Decrypt

For ease of details, we think that all primitives are implementing by the Tag. The actual set of rules involving the Tag, and Reader are explained in the after that section of set of rules.

- ✓ **Setup**:

We select a hyper elliptic curve C in excess of Z_p where, p is a prime number. We also represent 'g' as the

bottom point of E and 'h' as arrange of P, where k is also a point generate by the base point. Suppose g is (x, y).

Key invention

Our system selects the sender private key 'n' then we calculate h

$h = n(g) = n(x, y)$

By the group of element operation then we find h. suppose h is (x1, y1)

- ✓ **Encryption**:

Suppose m is a message it is form of points form. In the first message the Back-End sends broadcast "Hello" message in order to discover Tags near by the Reader. It is important to note that in our RFID model the Back-End and the system converts the message into ascii code. Then system converts ascii code into point.

Calculate

$$E_k(m,k) = (k(g)), m + k(h))$$
$$=(k(x,y), m+k(x1, y1))$$

Here suppose $a1 = k(x,y)$ and

$a2 = m+k(x1, y1)$

Send this encrypted message (a1, a2 by the sender or tags information.

- ✓ **Decryption**:

The decryption operation is perform by the receiver or reader.

Receive the message (a_1,a_2)

Decryption operation is

$D_k = a_2 – na_1$

So receiver or reader decrypt the message and find the real message.

V. SYSTEM MODEL IN OMNET++

The model consists of 3 separate parts: the first is the module, which simulates the behavior of the backend, the second simulates tags (Tag), which has multiple representatives in the system in the same time, and the third observer and data collecting module (Observer) stores the settings of the simulation and collects results of the measurement. The model is simpler than real systems, since it has no distinct reading module. The reading module would have only the task of managing communication between Back-End and Tag during the authentication process, in our case it is negligible. The model of the system can be seen in Figure 1

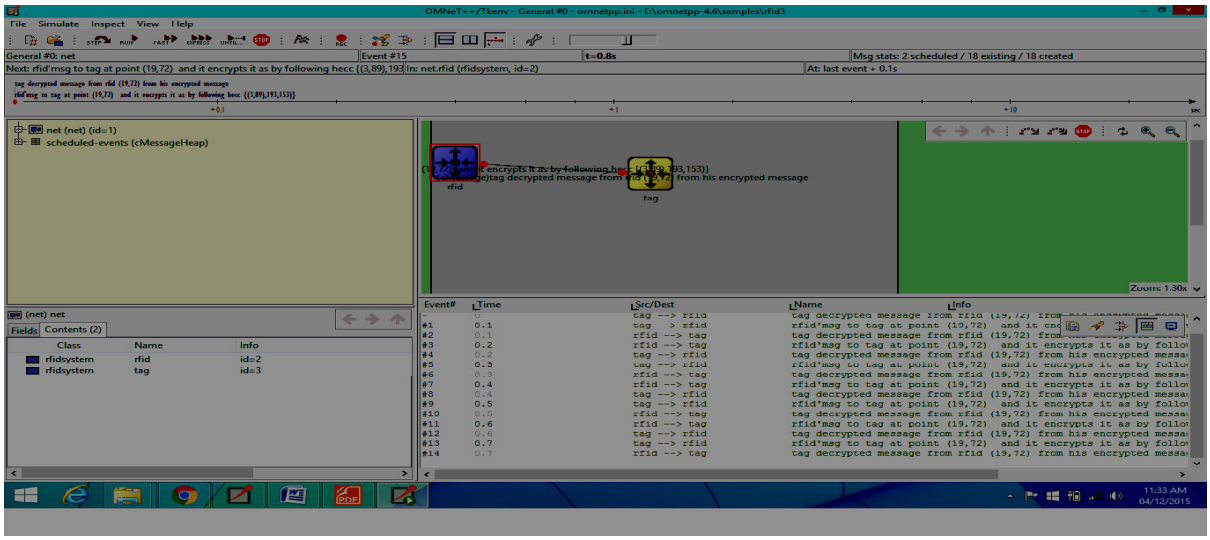

Figure 1 THE MODEL OF THE SYSTEM

VI. SECURITY AND PRIVACY ANALYSES

A. Tag tracking and tracing

In favor of RFID tags is intended to have an only one of its kind figure which can be trail in range of every readers. On the other hand, this procedure provides the instrument that whenever the fake reader inquiry the tag; the tag does not throw any answer reverse. Consequently, the tracking and tracing retreat is safe and sound in this procedure.

B. Replay attack

Replay attacks are the wireless network attacks in which an attacker tries the conversation among the sender and receiver and receive the authenticated information e.g. sharing key and after that contact to the receiver with that

key. In Replay attack the attacker gives the proof of his identity and authenticity. But our system use pair of points calculated by the curve so sender or receivers easily find out the unauthorized person.

C. **DOS (Denial of Service) attack**

A denial of service (DoS) attack is an occurrence in which a user or association is poor of the services of a resource they would usually expect to have. In a denial-of-service, structure attacks a single target. But our system use HECC algorithm. This algorithm .provide the security by the outside users

D. **Mutual authentication**

Mutual authentication, as well called cooperative authentication, is a process or equipment in which both thing in a communications relation authenticate each other. In a network environment, the tags authenticate the readers and vice-versa.

E. Information leakage

Data transmitted from first to last the air are simply compromised. In this procedure, there are exchange messages among the reader and the tag. These perceptive data are encrypted by HECC cryptographic Algorithm. The attackers can't gain the personal information or the untreated data. So the in a row leakage is negligible.

Table 1 comparison between different protocols from the point of analysis of security

Protocol	Proposed Prot.	ECC	ERAP	AES
Tracking	✓	✓	✓	✓
Replay Attack	✓	✓	✓	✓
DoS	✓	×	×	✓
Mutual Auth.	✓	✓	✓	✓
Information leakage	✓	✓	×	✓

VII RESULT ANALYSIS

In order to calculate the piece characteristics of our planned HECC protocol and to compose a comparison with further we implemented it and two other procedure in OMNeT++ [7]. The realization of the protocol is written on windows8 operating system in C++ programming language by using the GCC C++ compiler. The simulation was written in the Net.ned class environment and the program was debugged by using the GDB (GNU Debugger). The parameters of the Back-End as well as Tags are stored by using our system. As shown in the below table the comparative analysis of the base and the proposed work. The proposed technique realize here provides take away storage space cost and moreover the encryption as well as decryption time is take away.

Table 2 Timing Analysis of Proposed Work

Algorithm	ECC	HECC	% improvement
Key size	112, 160 and 256	16-256	-
Encryption and decryption time	0.00059ms	0.0001 Ms	83.05
Storage cost	Depends on key size	Depends on key size	-

Timing analysis of proposed work for RFID tag encryption and decryption time by the help of OMNeT++. This tool directly provide the tag encryption and reader decryption time.

VIII. CONCLUSION

Hyper elliptic curve cryptography provides security from various attacks in RFID devices. Also the planned methodology implemented here is efficient in terms of storage cost and computational time. The planned methodology implemented here is based on key invention using HECC and encryption is performed using identity of the tags. The result analysis shows the show of the planned technique. This can be achieved in small computational capacity environments. In addition, we implemented this protocol and others in OMNeT++, in order to compare them from the point of view of efficiency. It can be exposed that the performance of our method is equal or some cases better than the others.

IX. FUTURE ENHANCEMENT

ECC have been in extensive use since last decade, due to this ECC have standard domain parameters specified in the various standard document. HECC is fast due to its short operand size and providing the same level of security as ECC. Right now HECC doesn't have the standard domain parameter like that of ECC, may be some years later we will have the standard document for HECC DOMAIN PARAMETERS. So, as a future enhancement to the project we can enhance it by providing facilities for:

Domain parameter Invention: This will include invention of secure curve, point counting, and finding base point for the curve.

Domain parameter Validation: This will include validation of curve, point counting, and finding base

point for the curve, so that library should verify the input domain parameter before proceeding.

Graphical User Interface: After the above two enhancements will be complete, we can make use of SWING and develop a commercial secure software.

X. REFERENCES

[1] Farads Baghdadi, Charles Multiage and, "Research trend in RFID Technology", 2012, pp. 1-10.
[2] Liu Ya-li, "A Lightweight RFID substantiation Protocol based on Elliptic Curve Cryptography", JOC, VOL.8, 2013.
[3] Garfunkel, Simon and Beth, "RFID Applications defense, and Privacy", Addison-Wesley, pp.343, 2006.
[4], DR. Michael Kamuela, Jonathan Sangoro "Enhancement of protection in RFID using RSA Algorithm", IISTE, Vol 5, pp. 65-69, 2014.
[5] Dae Seo and Yeong Lee, "A Study on RFID System with protected Service Availability used for Ubiquitous Computing", IJIPS, Vol.1, No.1, 2005.
[6] Peter J. Hawraylak, Matthew Butler, John Hale, "Graceful Privilege decrease in RFID Security" , 2011 CSIIRW, Article No. 47, pp.47+12, Oct 2012..
[7]"OMNeT++, "http://www.omnetpp.org/. [Online]. Available: http://www.omnetpp.org/
[8] Tuan Pham,. Hasan and Hongnia Yu Mohammad S "A RFID mutual certification protocol based on AES Algorithm", IEEE, , pp. 997-999, 2012.
[9], V. Vijayalakshm and G. Zayaraz, P. Vijayakumar, "Comparative Study of Hyper elliptic Curve Cryptosystem over Prime pasture and Its Survey", IJHIT, vol. 7, pp. 137-146, 2014.
[10] Charles Mutagen and Far had Baghdadi, "Research Trend in RFID Technology",, pp 1-15, 2012.
[11] Tuan, Mohammad S. Hongnian Hasan, "A RFID mutual verification protocol based on AES Algorithm", IEEE, pp. 997-999, 2012.
[12], Norbert Gicczi, Gyozo God or, "Elliptic Curve Cryptography Based Mutual confirmation Protocol for Low Computational Capacity RFID Systems - Performance Analysis by Simulations", IEEE, pp. 650-657, 2010.
[13], Mustapha Djeddou , Karmic Drouiche , Mustapha Bensalem "Efficient ECC Implementation planning Suitable for RFID Technology" , IEEE, pp , 2012.
[14] Georgia, Kaiser Kang, Marietta, Yue Shi, "Research on Encryption representation Based on AES and ECC in RFID" IEEE, pp. 9-13, 2013.
[15] Dr. Hemalatha, A. Lemma, "A New Deferred cleansing system for Effective Warehousing of RFID" , EIT, pp. 626-631,2012.
[16] Ayman Kayssi Ali Chehab, Ramzi "A PUF-Based Ultra-Lightweight Mutual Authentication RFID procedure, "International Conference for Computing & Processing, pp. 495 – 499, 2011.