SHA-Based Mutual Authentication in Long Term Evolution Using Hyper Elliptic Curve Cryptography

P.Sandhya, S.Poovizhi, R.Varun

Abstract— Elliptic Curve Cryptography is used in Long Term Evolution (LTE) which uses large key size which fails to provide security against Denial of Services (DOS). In this paper, SHA-based mutual authentication is proposed for Long Term Evolution using Hyper Elliptic Curve Cryptography which is public key cryptography which helps in secure communication for exchanging the data. This reduces the communication complexity and computation cost using smaller key size which results in less processing time and provides security against DOS. Finally, simulation result shows the processing time between the ECC and HECC using MATLAB.

Index Terms— LTE, ECC, HECC, DOS

I. INTRODUCTION

A Wireless Mobile Communication technology has become more popular and easier to transmitting data for past years. Nowadays user can able to communicate with other parties at any place at any time. Long Term Evolution plays a major role in wireless communication.LTE system was designed to meet new technologies. Many algorithms were developed for secure communication.

Cryptography based authentication protocol was developed to guarantee the confidentiality, authentication and integrity of communications. Here very popular Hyperelliptic Curve Cryptographic technique is used to fulfill the requirement of LTE network to provide authentication between two users. These cryptographic technique provide security with less computational and communication overhead. It needs only 80bit key length to provide same level of security as ECC and RSA.

II. RELATED WORKS

"Secure Authentication Key Agreement Protocol for Long Term Evolution – Advanced"[1] describes that AKA protocol providing security against the vulnerability attacks."An Efficient protocol for resource constrained platforms using ECC" [5] describes that Elliptic curves were already being used in various cryptographic contexts. An elliptic curve exponentiation for general curves over arbitrary prime fields is roughly 5 to 15 times as fast as an RSA, depending on the platform and optimizations.

Manuscript received August 2013.

P.Sandhya, Electronics and Communication Engineering, Aksheyaa College of Engineering,Kancheepuram,India.

S.Poovizhi, Electronics and Communication Engineering, Aksheyaa College of Engineering, Kancheepuram, India.

R.Varun, Electronics and Communication Engineering, Aksheyaa College of Engineering, Kancheepuram, India.

"Elliptic Curve Cryptography and its applications" [7] describes that Elliptic Curve Cryptography (ECC) is a public key cryptography having a small key size of 160-bit in which each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. "Security Analysis and Enhancement of Authentication in CDMA based on Elliptic Curve Cryptography" [9] describes that Superiority of ECC public key technique over other public key techniques based on the key length and the implementation speed. CDMA Authentication technique used ECC public key to provide the subscriber Authentication key, and also provides Authentication request and Mutual Authentication between the user and service network.

III. EXISTING SYSTEM

Authentication key agreement algorithm is implemented for secrecy and to solve the vulnerabilities in the communication system. This reduces the bandwidth utilization for authentication and number of transactions required for authentication is reduced. Security and implementation requirements for personal communication systems has been discussed. To provide better protection, new protocols with more security features, which reduce the roamer's trust on a visited network's capability of protecting roamer-related sensitive data without involving complicated computations, are analyzed.

IV. PROPOSED MUTUAL AUTHENTICATION PROTOCOL

Mutual Authentication is necessary to avoid the intruder while transferring the information (or) messages. We propose a mutual authentication protocol based on "ISO-Public Key three phase mutual Authentication Protocol" in Long Term Evolution which provides high level of security in combination with Hyper Elliptic curve Cryptosystem. Proposed Protocol Postulates are as follows:

- Our Proposed mutual Authentication protocol based on "ISO public Key three pass mutual Authentication Protocol" in Long term Evolution as it used with Hyper Elliptic Curve which provide same level of security as 160-bit ECC.
- Authentication done using HEC-EIG algorithm which beneficial in less processing time.
- Key has been generated and signature has been added and verified using HEC-SHA algorithm which results in high level of security.

A. HEC-EIG Authentication

User A want to communicate with User B.So,User A sends a request message to User B containing User Identity (ID_A), Challenge nonce R_A and certificate $Cert_A$.Once the message received User B wants to communicate with A, it first verify the identity,if that matches User B sends message to User A which contains nonce R_B,ID_B and $Cert_B$.Now,User A and User B will communicate after the mutual authentication in fig 4.1

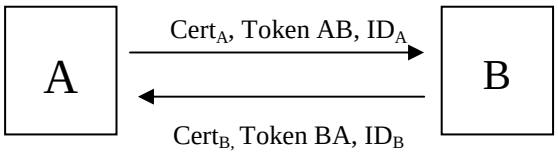

FIG.4.1HEC-EIG AUTHENTICATION

$$\text{Token AB}=R_A \| R_B \| B \| Sig_A (R_A \| R_B \| B)$$
$$\text{Token BA}=R_B' \| R_A \| B \| Sig_B (R_B' \| R_A \| A)$$

B. SHA-based Key Generation (User A)

1. Select random integer from [1; n-1]
2. Compute Q=d.p
3. A's public key is Q and private key is d.

C. Signature Generation (User A)

1. Random integer k from [1; n-1]
2. Compute k*G =(X_1; Y1); r = X_1(mod n)
3. If r=0 then go to step 1.
4. Compute [K ^ (-1)] [mod n]
5. Compute S= [K^ (-1)] [SHA -1(m) + dr] (mod n)
6. If S=0 then go to step 1
7. Send m and (r;s) which is A's signature for the message m, to B.

D. Signature Verification (User B)

1. Verify r and s
2. Compute e=SHA-1(m)
3. Compute w=[S^ (-1)] (mod n)
4. Compute U_1= [e * w] (mod n); U_2= [r * w] (mod n)
5. Compute $U_1P+ U_2Q=(X_1; Y1)$ and V=X_1(mod n)
6. If S=0, then go to step 1.
7. Accept the signature if and only if V=r.

TAB 4.1 KEY Exchanging And Verifying

STEP	USER A	USER B
1	Key Generation Q=d.P Public Key:Q Private Key:d r=X_1(mod n) S=[K^ (-1)] [SHA -1(m)+dr] (mod n)	
2	→	$U_1P+U_2Q=(X_1;Y_1)$ V=X_1(mod n) All Condition satisfied accepted V=r ←

E.Protocol

1. User A generates the private key (d) and public key (Q)
2. Computation of signature generation is,
   S=[K^ (-1)] [SHA -1(m)+dr] (mod n)
3. Verify User B,check the parameter with computation V=r.

V. SIMULATION RESULTS AND DISCUSSION

MATLAB simulation tool was used to simulate the proposed cryptographic scheme for different key size and processing time. Fig.5.1 shown the simulated result by comparing key size and processing time for ECC and HECC .From the results it was inferred that ECC takes more processing time than HECC. For key size of 100 bits, ECC takes processing time of 960ms whereas HECC takes only 180ms. From the simulated graph, it is inferred that as key size increases, the processing time for ECC increases whereas the processing time for HECC decreases.

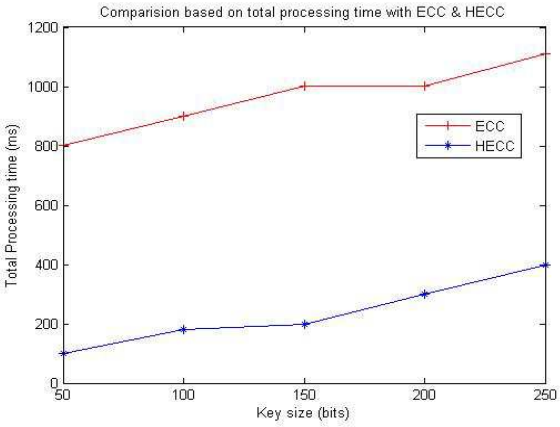

Fig.Key Size Vs Processing Time

V. CONCLUSION

This paper describes a novel cryptographic scheme with HECC algorithm on LTE for secure data exchange. This proposed method offers major advantages over traditional systems such as increased speed, less memory and smaller key size. It also provides higher level of security with less key size of HECC-80 bits than ECC-160 bits.

REFERENCES

[1] M. Prasad and R. Manoharan "Secure Authentication Key Agreement Protocol for Long Term Evolution – Advanced", Elsevier Journal, Department of Computer Science and Engineering, Puducherry.

[2] S. Prasanna Ganesan: "An Efficient Protocol for Resource Constrained Platforms Using ECC",Vol.2 (1), 2009, pp. 89-91. www.enggjournals.com/ijcse/doc/IJCSE10-02-01-16.pdf.

[3] William Stallings, "Cryptography and Network Security", Principals and Practices, Pearson edition (India) Pvt.ltd, 4th Edition, 2009.

[4] Moncef Amara and Amar Said, "Elliptic Curve Cryptography and its applications", Issue Date: 9-11 May 2011, pp. 247-250, Date of Current Version: 27 June 2011.

[5] S. Prasanna Ganesan, "An Authentication Protocol For Mobile Devices using Hyper Elliptic Curve Cryptography", *in the ACEEE proceeding of* International J. of Recent Trends in Engineering and Technology, vol.3, No. 2, May 2010.

[6] Mohammed A, Mahdi, "Security Analysis and Enhancement of authentication in CDMA based on Elliptic Curve Cryptography", in the proceedings of Information journal of research technology.

[7] Sameer Hasan Al-Bakri, M.L. Mat Kiah, A.A. Zaidan, B.B.Zaidan, Gazi Mahabubul Alam: Securing peer-to-peer mobile communications using public key cryptography: New security strategy, Vol.6(4),pp.932-938, 18 February 2011.

[8] Sukalyan Goswami, Subarna Laha, "Enhancement of GSM Security Using Elliptic Curve Cryptography",2012 International Conference on Information Technology and Computer Science, Department of Electronics and Computer Science, Kolkata, India.

[9] Jeremy Quirke,. Henri Cohen, Gerhard Frey, Chapman and Hall/CRC, "Security in GSM System", Taylor and Francis, Florida, 2004.

[10] Tuan Huynh and Hoang Nguyen: "Overview of GSM and GSM Security" Department of Electrical Engineering and Computer Science Oregon State University June 06, 2003.