A Review: Elliptical Curve Cryptography in Wireless Ad-hoc Networks

A.Naveena[1], Dr.K.Ramalinga Reddy[2]

[1]*Assistant proferrsor, ETM Dept, G.Narayanamma institute of Engineering and Technology for Women*
[2]*Dr.K.Ramalinga Reddy, HOD, ETM Dept, G.Narayanamma institute of Engineering and Technology for Women*

---***---

Abstract - *As the wireless industry exploding, the need for security is also exploding. Both for secure communication between two parties, Web transactions and for secure messaging, efficient Public Key Infrastructure is needed. Elliptic Curve Cryptography (ECC) is a recent branch of cryptography based on the arithmetic of elliptic curves and the Elliptic Curve Discrete Logarithm Problem (ECDLP). Elliptic curve cryptographic schemes are public-key mechanisms that provide encryption, digital signature and key exchange capabilities. ECC provides better security for wireless ad-hoc networks compare to other cryptographic techniques because of its small key size. In this survey, we are enhancing the role of elliptical curve cryptography in wireless ad-hoc networks.*

Key Words: encryption, decryption, elliptical curve cryptography (ECC), MANET (Mobile Ad hoc Network), multi hop network, VANET (Vehicular Ad hoc Network), multi hop network ECKCDSA (Elliptic curve Korean Certificate Based Digital Signature Algorithm).

1. INTRODUCTION

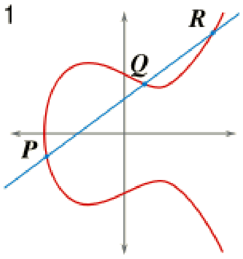
A wireless ad hoc network (WANET) is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks [7] or access points. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity.

Wireless ad-hoc networks can be further classified by their application. [7]A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. VANETs are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (In VANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents.

Security is being a major threat in information sharing through networks.[4] For making the information secure in the existing system ECC is used because of its small key size. Cryptography is an electronic technique .It is used to protect valuable data while communicating. The main objective of cryptography is to protect our data by using different authentication schemes. Two main terms that is used for the cryptography technique are Encryption and Decryption. Encryption technique is used to send confidential data over communication. Decryption is the reverse process of encryption. It is technique to convert the encrypted data to its original data that is now readable [1].

ECC is emerging as an attractive public-key cryptosystem for mobile/wireless environments. Compared to traditional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, faster computation, lower power consumption, as well as memory and bandwidth savings.

The[3] mathematical operations of ECC is defined over the elliptic curve **y2 = x3 + ax + b,** a and b are elements of a finite field with p^n elements, where p is a prime number which is selected as larger than 3.The set of points on the curve is the collection of ordered pairs (x, y) with coordinates in the field and such that x and y satisfy the relation given by the equation **y 2 = x3 + ax + b** defining the curve, plus an extra point that is said to be at infinity.



$$y^2 = x^3 + ax + b$$

The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters "a" and "b", together with few more constants constitutes the domain parameter of ECC.[2] One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

2. ECDSA - Elliptic Curve Digital Signature Algorithm

ECDSA [1] is a variant of the Digital Signature Algorithm (DSA) that operates on elliptic curve groups. For sending a signed message from Alice to Bob, both have to agree up on Elliptic Curve domain parameters (D). For authentication of a message Alice signs the message using her private key. This signature can be verified only by using the public key of Alice. Since Bob knows Alice's public key, it can verify whether the message is indeed send by Alice or not.

ECDSA process is defined below:

Alice
Parameters D = (q, a, b, G, n, h)
Associated keys (d, Q)

To sign message m:

1. k randomly chosen $0 < k < n-1$
2. $k \cdot G = (x_1, y_1)$ $r = x_1 \bmod n$
3. if $r = 0$ abort and start again
4. e = SHA-1(m)
5. $s = k^{-1} \cdot (e + d \cdot r) \bmod n$
6. if $s = 0$ abort and start again

Output: (r, s)

Bob
Parameters D = (q, a, b, G, n, h)
Alice's public key Q
Alice's signature (r, s) on m.

To verify signature (r, s):

1. check: $1 \leq r \leq n-1$, $1 \leq s \leq n-1$
2. e = SHA-1(m)
3. $w = s^{-1} \bmod n$
4. $u_1 = e \cdot w \bmod n$ $u_2 = r \cdot w \bmod n$
5. $X = u_1 \cdot G + u_2 \cdot Q$, if
6. $X=(x_1, y_1)$ $v = x_1 \bmod n$
7. Accept if v=r

1.2. ECDH - Elliptic Curve Diffie Hellman

ECDH is a key agreement [1] protocol. A shared secret key is established and that can be used for private key algorithms. For generating a shared secret between Alice and Bob using ECDH, both have to agree up on Elliptic Curve domain parameters.
An overview of ECDH process is defined below:
Alice and Bob compute their public and private keys.

Alice
Private Key = X
Public Key = $P_A = X * B$

Bob
Private Key = Y
Public Key = $P_B = Y * B$

Alice and Bob send each other their public keys. Both take the product of their private key and the other user's public key.

Alice → $K_{AB} = X (YB)$
Bob → $K_{AB} = Y (XB)$

Shared Secret Key = $K_{AB} = XYB$

3. ECIES -Elliptic Curve Integrated Encryption Scheme

Now-a-days Vehicular Ad-hoc Networks (VANET) are becoming more popular.[9] The accident rates are increasing day-by-day because they have limited opportunities to communicate each other due to their high speed. Many attacks in this network can be prevented or detected using cryptography methods. The most extended encryption and decryption scheme based on ECC is called the Elliptic Curve Integrated Encryption Scheme (ECIES).

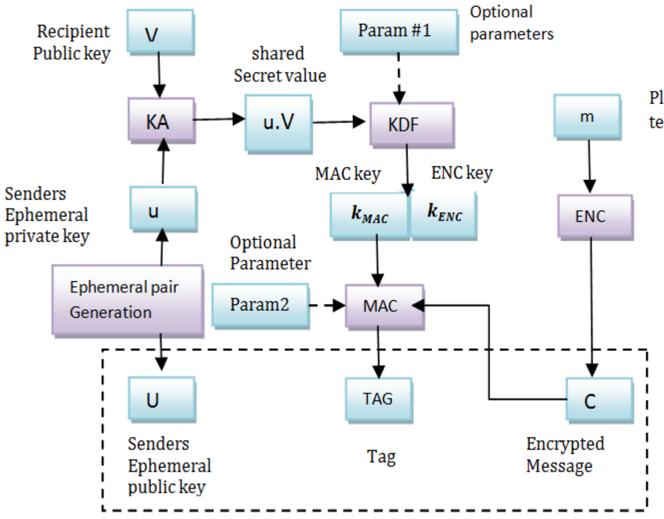


Fig 3.1 Encryption by Alice

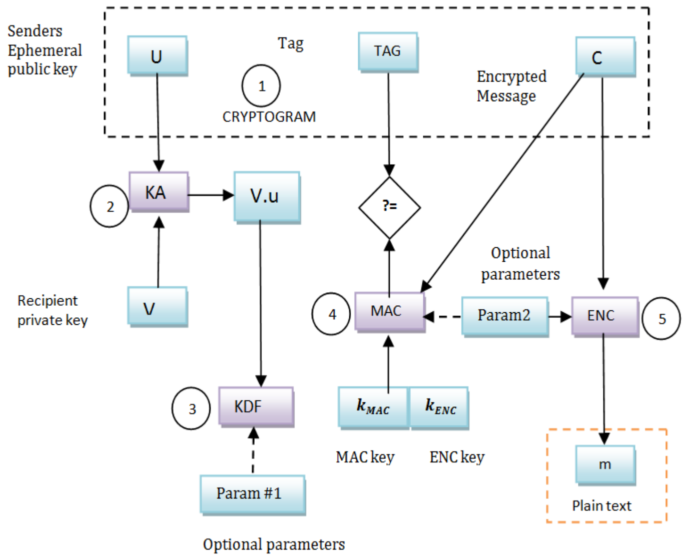


Fig 3.2 decryption by Bob

The above figures are referred from [9].

4. ECC Based Key Agreement Protocol

Based on the elliptic curve[1][6] DL assumption a new energy efficient two parties mutual authenticated key agreement protocols suitable for MANET was proposed. This scheme has used Hybrid Crypto Token (HCT) for computational efficiency. It uses two different cryptographic primitives such as

1. ECC (key pair of MANET node uses ECC)
2. RSA (key pair of TTP is uses RSA)

There are two phases of this Two-Party Authenticated key Agreement Protocol

i. Registration Phase
ii. Active Phase

Registration Phase: In this phase Trusted Third Party (TTP) issues a certificate known as HCT to registered MANET nodes. This phase uses RSA primitives, especially for computing the digital signature during generation of HCT.
Active Phase: To conserve the energy of resource constrained MANET nodes, this phase uses ECC-based PKC primitives for generating key pair and symmetric key among MANET nodes and also for generating and verifying signature during authenticated key agreement process.

1. Node A after receiving the node B's beacon verifies its HCT sends an authentication request
Node A also generate random RNA

2. Node B verifies the A's token using public key of TTP, verification is successful, generates RNB and computes SKBA as a session secret key between A and B.

3. Node B computes It then constructs a message m consists of RNA, RNB, QB and HMACB, that is,
m = RNA||RNB ||QB||HMACB and generates a signature sigB(m) on m as sigB(m) = (r, s) using the private long-term key b of B with the help of ECDSA signature generation algorithm. Node B finally sends ARep (m, sigB(m)) as an authentication reply message to node A.

4. Node A after receiving ARep verifies signature sigB(m) using public key of node B with help of ECDSA signature verification algorithm further it checks whether RNA = ? Previously generated RNA.If both RNA are equal node A computes session secret key SKAB = H ((rA+a). (QB+PubB) ||IDA||IDB||RNA||RNB)

5. Node A compares computed HMACA with received HMACB for integrity check. If integrity check holds, as an initiator node A ensures successful execution of authenticated key agreement protocol with node B.

6. Node A sends an acknowledgement (RNB||HMACA)||sigA(RNB||HMACA) to node B. Node B after receiving acknowledgement ,verifies A‟s signature sigA(RNB||HMACA) using public key of node A ,If this verification holds it checks whether RNB =? Previous RNB and received HMACA =? Previous HMACB. If these hold, it stores SKBA for secure communication with A.

5. Modified ECC with ECKCDSA (Elliptic curve Korean Certificate Based Digital Signature Algorithm) based on SHA 512 hash function

The problem of using MANET connections is based on security. [8]MANET does not have any safe security policy, so there is a chance for attackers to easily destroy the mobile network topologies. To discover the attackers and also to find its effects, a new hybrid based algorithm named ECKCDSA with SHA 512 hash function is proposed.

The aim of ECKCDSA SHA512 hash function is to improve the detection of the misbehavior nodes which is attacking by enhancing the system security.

Signature Generation:

1. Select a unique integer X in the interval [1,n-1]
2. Xg ← (a,b), where a is an integer
3. r ← a mod n; If r = 0, then go to step 1
4. h ← H(z || M), where H is the SHA-512
5. s ← d(X - r xor h) mod n; If s = 0, then go to step1
6. The signature of Alice for message M is the integer pair (r,s)

Signature Verification:

Bob can verify the authenticity of Alice's signature (r, s) for message M by performing the following:

1. Compute e= Hash(hcert ‖m)
2. Compute the integer w = r xor e(mod n)
3. Compute X=(x1,y1) = wG+sDA
4. If X=0, reject the signature.
   Otherwise compute v= Hash(x1) mod n
5. Finally check and accept the signature only if r= v.

CONCLUSION

Security is the important aspect in present world. Wireless devices are becoming popular now-a-days. As the increase in their popularity also increasing the need for security such as the ability to do secure email, secure Web browsing, and virtual private networking to corporate networks. Past years, ECC is providing more efficient implementation of all of these features. Compare to first generation techniques, ECC provides greater technique with its small key size. The vital role of ECC for the mobile ad-hoc networks are seen here. In future, the extension of these ECC cryptographic techniques can provide great secure, efficient and fast communication.

REFERENCES

[1] E.Thambiraja, Dr. R.Umarani, G.Ramesh," A Survey of the Elliptic Curve Integrated Encryption Scheme", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012.

[2] Kristin Lauter,Microsoft Corporation,2004, "The Advantage of Elliptic Curve Cryptography For Wireless Security",IEEE Wireless Communications

[3] Certicom, Standards for Efficient Cryptography, SEC 1:" Elliptic Curve Cryptography, Version 1.0, September", 2000.

[4] http://www.dkrypt.com/home/ecc#TOC-EC-Cryptography

[5] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[6] Enge, A. Elliptic Curves and Their Applications to Cryptography. Springer Verlag. 1999.

[7] Evans, J., Wang, W., & Ewy, B. (2006). Wireless networking security: open issues in trust, management, interoperation, and measurement. International Journal of Security and Networks (IJSN), vol.1, no. ½ (pp.84-94).

[8] M.CHARLES AROCKIARAJ, Dr.P.MAYILVAHANAN," Overhead minimization in manet using improved elliptical security algorithm" International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-2, Issue-1,January 2016

[9] V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila" A Survey of the Elliptic Curve Integrated Encryption Scheme" journal of computer science and engineering, volume 2, issue 2, august 2010