ELLIPTIC CURVE INTEGRATED ENCRYPTION SECEME USING ANALYSIS VEHICULAR AD HOC NETWORK

Dr. E. Balamurugan, M.Sc., M.Phil., PhD
Associate Dean, Accra, Ghana
balamurugan@Bluecrest.edu.gh

Abstract: A network connection is created for single session and not involves a router or a wireless base station. Vehicular ad hoc network (VANET) is an application of mobile network. VANET is a self-organized network and it is used for communicate between vehicle and road side units. The main objective is improving driving safety and managing traffic with internet access by programmers and drivers. Here every car it acts as a router or node and network range of 100 to 300 meters. If car signal is dropping a network the other remaining vehicles or node can merge to the ad hoc network and create a mobile internet but it not rely on preexisting infrastructure. In this technology main goal is provide communication between one vehicle or node to another vehicle or node to protect the road safety and provide secure communication. There are many types of encryption and decryption methods are used in this environment. In this paper, discuss about the many types of security algorithms in vehicular ad hoc network and its feasible solutions by using ECIES cryptographic scheme.

Keywords: *Encryption, Decryption, Authentication, SSL &SSH, RSA Encryption/Decryption scheme, ECC Elliptic Curve Integrated Encryption scheme.*

1. INTRODUCTION

Vehicular Ad hoc Networks is a special kind of mobile ad hoc network to provide communication among nearby vehicles and between vehicles equipment's . It is mainly used for improving efficiency of vehicles and safety of (future) vehicles. There are number of possible attacks in VANET due to open nature of wireless medium. This security attacks and logically organized/represented in a more lucid manner based on the level of effect of a particular security attack on intelligent vehicular traffic.

Network security

It consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification, misusing, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users select or are allocated an ID and password or other authenticating information that permits them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in day by day jobs conducting transactions and communications among businesses, government agencies and individuals.

Networks can be private, for example within a company, and others which could be open to public access. Network security is involved in organizations, enterprises, and another types of institutions. It secures the network with protecting and overseeing operations are completed. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password [1].

2. PERFORMANCE COMPARISON OF ECC AND RSA ENCRYPTION SCHEMES

Rob Shaw and Yin (1997) compared the operational characteristics of RSA and ECC. In their article, they claimed that assuming all necessary parameters and with ECC will be almost 8 times longer than with RSA, and decryption will be almost 6 to 7 times faster[2]. These findings, however, contrasted that of Certicom Corporation who adjudged the most efficient implementation of ECC 10 times faster than comparable RSA systems [3].

2.1 Theory of RSA Cryptosystem

The RSA is the most widely used cryptosystem today. Unfortunately, encrypting a message, m, involves exponentiation, $C= m^{e} \bmod n$, a mathematical procedure which requires a lot of computations, making it impossible to achieve the speeds of private key systems such as DES, a phenomenon that is true for all public key systems[4].

To set up a RSA cryptosystem, a user (say Alice) picks two large primes p and q and computes their product, n= p q . The group used is the multiplicative group (g=z*) of units in the integer modulo n. It is well known that the order of G is ***φ=(p-1)(q-1)***, where *φ* denotes the

Euler phi function. Clearly, Alice's public key is the pair of integers {n, e} and her private key is d.

2.2 RSA Key Generation

An RSA key pair can be generated using key pair generation Algorithm. The public key consists of a pair of integers (n, e) where the RSA modulus n is a product of two randomly generated (and secret) primes p and q of the same bit length. The encryption exponent e is an integer satisfying $1 < e < φ$ and gcd (e, φ) = 1 where $φ = (p−1)(q −1)$. The private key d, also called the decryption exponent, is the integer satisfying $1 < d < φ$ and $ed ≡ 1 \pmod φ$.

It has been proven that the problem of determining the private key d from the public key (n, e) is computationally equivalent to the problem of determining the factors of p and q.

2.3 RSA key pair generation

INPUT: Security parameter l.

OUTPUT: RSA public key (n, e) and private key d.

- Randomly select two primes p and q of the same bit lengthl/2.
- Compute n = pq and φ = (p−1)(q −1).
- Select an arbitrary integer e with 1 < e <φ and gcd (e, φ) = 1.
- Compute the integer d satisfying 1 < d <φ and ed ≡ 1 (mod φ).
- Return (n, e, d).

2.4 RSA Encryption/ Decryption Scheme

RSA encryption schemes use the fact that **med ≡ m (mod n)** for all integers m. The encryption and decryption procedures for the (basic) RSA public-key encryption scheme are presented as basic RSA encryption and decryption Algorithms.

Decryption works because cd ≡ (me)d ≡ m (mod n), as derived from expression. The security relies on the difficulty of computing the plaintext m from the cipher text c = me mod n and n and e are public parameters . This is the problem of finding e-th roots modulo n and is assumed (but has not been proven) to be as difficult as the integer factorization problem [6].

2.4.1 Basic RSA encryption:

INPUT: RSA public key *(n, e)*, plaintext $m \in [0, −1]$. **OUTPUT:** Cipher text *c*.

- Compute $c = me \bmod n$.
- Return(c).

2.4.2 Basic RSA decryption:

INPUT: RSA public key *(n, e)*, RSA private key *d*, cipher text *c*.

OUTPUT: Plaintext *m*.

- Compute $m = c^{d} \bmod$
- n. Return (m).

2.5 Comparison between ecc and rsa

To test and compare the performance characteristics of the RSA and ECC encryption algorithms, we independently tested each of the following three main components for timings: key generation, encryption and decryption. Timings are not absolute so each operation for every test parameter was run 20 times in order to reach satisfactory level of confidence interval.

A 99.9% confidence interval was calculated from the test results using the student T-distribution. We also measured the size of the data files used to store the encrypted results.

2.5.1 The parameters of the operations are:

- The size of the applied key.
- The size and content of the input data.

Tests were performed on Intel Pentium dual core 1.6GHZ machine with 512MB of RAM. The message used for encryption is the 100 byte text. ECDLP is considered to be harder than both the Discrete Logarithm Problems and Integer Factorization.

Estimates are given for parameter sizes providing comparable levels of security for RSA and EC systems.

The parameter sizes, also called key sizes, that provide equivalent security levels for RSA and EC systems are as listed in Table 1.

Table 1: Comparable key sizes between ECC and RSA

ECC	RSA
160	1024
224	2048
256	3072
384	7680
512	15360

3. ELLIPTIC CURVE INTEGRATED ENCRYPTION SYSTEM (ECIES)

Integrated Encryption Scheme (IES) is a hybrid encryption scheme that provides semantic security against an adversary who is permitted to use chosen-plaintext and chosen-cipher text attacks. The security of the scheme is depends on the Diffie–Hellman problem. The elliptic curve incorporated encryption system (ECIES) is the standard elliptic curve based on encryption algorithm. It is called integrated, since it is a hybrid scheme that applies a public key system to transfer a session key for use by a symmetric cipher. ECIES is a public-key encryption algorithm.
To send an encrypted message to Bob using ECIES

3.1 Alice requires the following information:

- Using cryptographic suite:
  - ✓ KDF
  - ✓ MAC
  - ✓ symmetric encryption scheme E
- EC domain parameters(p, a, b, G, n, h) for a curve over prime field or (m, f (x), a, b, G, n, h) for a curve over binary field;
- Bob's public key: KB(Bob generates it as follows: KB = KBG , where KB is the private key he chooses at random: KB€ [1, n-1]
- Optional shared information: S1 and S2.

3.2 To encrypt a message m Alice does the following:

- It generates a random number r € [1,n-1] and calculates R = rG;
- we can derives a shared secret: S = Px, where P = (Px, Py) = rKB (and $P \neq 0$)
- It uses KDF to derive a symmetric encryption and a MAC keys: KE || KM = KDF(S||S1);
- It can be encrypts the message: c = E(KE; m);
- It can computes the tag of encrypted message and S2: d = MAC(KM; c||S2); outputs R||c||d.

3.3 To decrypt the cipher text R||c||d Bob does the following:

- It can be derives the shared secret: S = Px , where P = (Px, Py) = KBR (it is the same asthe one Alice derived because P = KBR = KBrG = rKBG =rKB), or outputs *failed* if P = 0;
- We can derives keys the same way as Alice did: KE||KM = KDF (S||S1);
- It uses MAC to check the tag and outputs *failed* if $d \neq$ MAC(KM ; c||S2);
- It uses symmetric encryption scheme to decrypt the message m = E -1(KE; c)

4. PROPOSED SYSTEM

A process of converting Plain Text into Cipher Text is called as Encryption. A reverse process of encryption is called as Decryption.

To overcome the problems in Elliptic Curve cryptography is to provide the requirements:

- Security is difficult
- Size of elliptical curve cryptography
- Discrete log the problem
- Intractability of certain mathematical problem

In existing several algorithms or techniques are used for encryption and decryption it will be produce better result. In proposed system will be implemented by using ECIES with C++ it provides more security than previous one encryption and decryption methods.

5. CONCLUSION AND FUTURE WORK

Public-key encryption can be used to eliminate problems involved with conventional encryption. However, it has not managed to be as widely accepted as conventional encryption as it introduces a lot of overheads. Consequently, it is very important to get ways to reduce the overheads yet not sacrificing on other features of security so that the desirability in public key can be exploited.

After comparing the RSA and ECC ciphers, the ECC has proved to involve much less overheads compared to RSA. The ECC has been shown to have many advantages due to its ability to give the similar level of security as RSA yet using shorter keys. But, its disadvantage that may even hide its attractiveness is its lack of maturity, as mathematicians believed that enough research that has been compare to ECC is better than ECIES for encryption and decryption for security.

There are several techniques and algorithms implemented in MANET and as well as in VANET too they are: RSA algorithm, diffie-hellman Algorithm and Elliptic Curve Integrated Encryption System. By using Elliptic Curve Integrated Encryption System it can provide security at minimum level.

In future it can be implemented by using ECIES with C++ with the help of NS2 simulator tool or MAT LAB.

REFERENCES

[1] http://en.wikipedia.org/wiki/Network security

[2] Rob shaw, M . J. B. and Y. L. Yin (1997),"Elliptic CurveCryptosystems', Http://www.rsasecurity .com/rsalabs/ecc/elliptic curve.html.

[3] Stallings, W. (2003)," Cryptography and Network Security: Principles and Practice", 3rd edition, PrenticeHall, New Jersey .

[4] Brown, M ., D. L. Hankerson, J.L_opez and A. M enezes (2001), "Software implementation of the NIST Elliptic curves over prime fields. In Progress in Cryptology - CT-RSA, D. Naccache", Ed., vol. 2020of Lecture Notes in Computer Science, pp . 250-265.

[5] Certicom Corp ., (2004), "An elliptic curve cryptography (ecc)primer,White paper, erticom.

[6] Weil, N. (1998)," U.S. govt.'s encryption standard cracked in record time: Network World". http://www.networkworld.com/news0720des.html