Elliptic Curve Cryptography Enabled Security for Wireless Communication

C. SAJEEV*
Research Scholar, Department of MCA, Sathyabama University
Jeppiaar Nagar, Rajiv Gandhi Road,
Chennai – 600 119, Tamil Nadu, INDIA
painkulamcsajeev@yahoo.co.in

G. JAI ARUL JOSE
Research Scholar, Department of MCA, Sathyabama University
Jeppiaar Nagar, Rajiv Gandhi Road,
Chennai – 600 119, Tamil Nadu, INDIA
aruljose@yahoo.com

Abstract: **Neal Koblitz and Victor Miller independently proposed elliptic curve cryptography (ECC). This is an efficient technique, which provides security for wireless communication. Earlier we were using wired equivalent privacy (WEP) protocol and Rivest-shamir-Adleman (RSA) scheme, which largely stimulated the research and development of security protocols for wireless communication. The efficient technique elliptic curve cryptography overcomes the disadvantages of WEP and RSA. Here we are proposing a mutually authenticated key agreement protocol that employs elliptic curve digital signature algorithm (ECDSA) exchange used for mutual authentication and key exchange respectively. The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size thereby reducing processing overhead. The proposed protocol can be implemented in both basic service set (BSS) and extended service set (ESS).**

Keywords: Elliptic Curve, Cryptography, Network Security, Wireless Technology, Wireless Communication

1. INTRODUCTION

In wireless mobile communication technology and personal communication systems, open air is used as communication channel, the content of communication may exposed to an eavesdropper or system services can be used fraudulently. So to provide security over wireless communication channel, security measures such as confidentiality, authenticity need to be provided. In general symmetric encryption algorithms are used to obtain high data rates. These algorithms use identical keys for encryption and decryption. The key exchange problem is the major flaw of using symmetric algorithms. The key must be exchanged between the two communication parties and ensure that key remains secret. Asymmetric encryption algorithms solve these problems. They replace the single shared secret key with a pair of mathematically related keys: one public key that can be made publicly available and one secret private key. All asymmetric algorithms have in common that they rely on the special properties of one-way function, but without additional information it's nearly impossible to calculate the inverse function. Traditional asymmetric algorithms utilize the multiplication of huge prime numbers as one-way function. Another method suggests the use of special operations with elliptic curves as one-way functions. These methods are called Elliptic Curve Cryptography.

To meet today's needs for wireless digital communication. The developed protocol needs to be highly secure, requiring low computational overhead and thus low power. Here, we introduce new authentication and key agreement protocol for wireless mobile communication system. The protocol is based on elliptic curve cryptography. Due to design flaws in WEP, wireless communication lacks the security attributes and becomes vulnerable to both active and passive attacks.

2. RELATED WORKS

We proposed an authenticated key agreement protocol that offers mutual authentication and secured way of deriving a shared secret key where both the entities contribute information for key agreement.

A. Wired Equivalent Privacy(WEP)

Anyone with a radio receiver can eavesdrop on a wireless local area network (WLAN) , and therefore widely acknowledged that a WLAN needs a mechanism to counter this threat. The IEEE 802.11 standard defines a data confidentiality mechanism known as Wired Equivalent Privacy (WEP). The security goal of WEP is data confidentiality equivalent to that of a wired LAN. When WEP is active in wireless LAN, packet is encrypted separately with RC4 cipher stream generated by a 64-bit RC4 key. The 64-bit key consists of a 24-bit initialization vector and a 40-bit WEP key. The encrypted packet is generated with a bit wise exclusive OR of the original packet and RC4 stream. The initialization vector chosen by the sender should be changed so that every packet won't be encrypted with the same cipher stream. A 4-byte integrity check

value is computed on the original packet using CRC32 checksum algorithm.

Problems with WEP

• 24-bit IVs are too short, and this puts confidentiality at risk.
• The CRC checksum, called the Integrity Check Value (ICV), used by WEP for integrity protection is insecure, and does not prevent adversarial modification of intercepted packets.
• WEP combines the IV with the key in a way that enables cryptanalytic attacks. As a result, passive eavesdroppers can learn the key after observing a few million encrypted packets.
• Integrity protection for source and destination addresses is not provided.

B. RSA

The RSA algorithm, invented by Rivest, Shamir, and Adleman , is one of the simplest public-key cryptosystems. The parameters are *n, p* and *q, e,* and *d.* The modulus *n* is the product of the distinct large random primes: *n = pq.* The RSA algorithm can be used to send encrypted messages and to produce digital signatures for electronic documents. The RSA algorithm requires computation of the modular exponentiation which is broken into a series of modular multiplications by the application of exponentiation heuristics.

Problems with RSA

1 The key length for RSA is greater.
2 RSA algorithm results in processing overhead.
3 Since RSA uses 1024bit keys, it reduces the overall system security strength to

80bits whereas the total strength required is 128bits.
4 To support this strength RSA requires a minimum key size of 3072bits.
5 Time consumption is more.

C. Elliptic Curve Cryptography

ECC stands for Elliptic Curve Cryptography. It contains certain advantages.

ECC devices require less storage, less power, less memory, and less bandwidth than other systems. This allows you to implement cryptography in platforms that are constrained, such as wireless devices, handheld computers, smart cards, and thin-clients. It also provides a big win in situations where efficiency is important. For example, the current key-size recommendation for legacy public schemes is 2048 bits. A vastly smaller 224-bit ECC key offers the same level of security. This advantage only increases with security level—for example, a 3072 bit legacy key and a 256 bit ECC key are equivalent—something that will be important as stronger security systems become mandated and devices get smaller.

3. ELLIPTIC CURVES

An elliptic curve is a set of points in the equation. $Y^2=x^3+ax+b$ where a&b are real numbers and x and y take on values in real numbers. Such equations are said to cubic because the highest exponent they contain is 3. Using the above equation we have to plot the elliptic curve. If three points in an elliptic curve lie in a straight line then their sum is O. The negative of point p is the point with the same x coordinate but the negative of the y coordinate; that is, if p=(x,y),then –p=(x,-y).note that these two points can be joined by a vertical line. Note that p+ (-p) =p-p=O.

To add two points P and Q with different x coordinates, a straight line is drawn between them and find the third point of intersection R. To form a group structure, we need to define addition on these three points as follows: P+Q= -R. we define P+Q to be the mirror image of the third point of intersection.

Let $P(x_1, y_1)$ and $Q(x_2, y_2)$ be elements of the ECG.
Then $P + Q = (x_3, y_3)$, where

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$x_3 = \lambda^2 - x_1 - x_2$$

And

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & if \quad P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & if \quad P = Q \end{cases}$$

The points on the elliptic curve should satisfy the equation

$$Y^2 \bmod p = (x^3 + ax + b) \bmod p$$

4. ECC BASED ALGORITHMS

We have used Elliptic curve Elliptic curve digital signature algorithm (ECDSA) for authentications respectively.

A. ECDSA

The elliptic curve adaptation of digital signature algorithm is called as ECDSA. The message to be sent is first hashed by SHA-1 algorithm to generate a message digest. It is then passed through the signature generation algorithm to generate the signature of the message. Receiver then passes the message through the same hash algorithm and then uses the signature verification algorithm to verify the signature. If the message is verified successfully receiver authenticates the sender. In the following, *H* denotes a cryptographic hash function whose outputs have bit length no more than that of *n*.

5. PROPOSED PROTOCOL

The figure1 shows proposed key agreement (KA) protocol. Let the authentication process involves two entities A and B. let entity A and entity B generate a random integers x and y. These are known as private keys. Then both the entities calculate their public keys X, Y by the scalar multiplication of their private key and shared generating base points. Our protocol starts with entity A sending X to entity B. entity B in turn responds with Y in concatenation with signature of received X. and finally entity A transmits the signature of both X and Y in concatenation. The general model of protocol is implanted into the BSS and ESS network respectively.

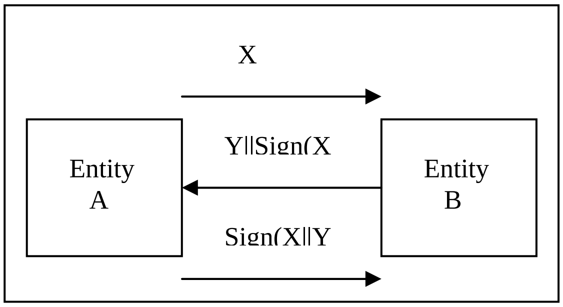

Figure 1: Proposed Three-Pass KA Protocol

A. BSS Network

In BSS networks, after the reception of the authentication request sent by the STA, AP will start the KA protocol and depending on the verification, success/failure messages will be sent to the STA as shown in fig.2. In case the STA detects the failure of the authentication process with the AP, it silently discards the session. All the messages used by the KA protocol for BSS network uses WLAN format.

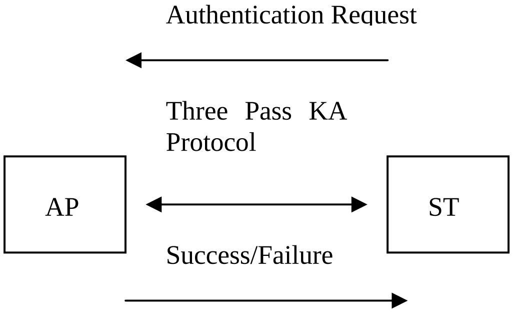

Figure 2: Message exchange of KA in

B. ESS Network

The proposed protocol in ESS network is fully compatible. Here we have only one server called RADIUS server and many clients. A fixed key is stored in the RADIUS server. One client can communicate with other client using the key available with RADIUS server used for encryption and decryption. The same key is used for all other client to client communication.

6. CONCLUSIONS

ECC is such an excellent choice for doing asymmetric cryptology in portable, necessarily constrained device right now. As an example, a popular, recommended RSA key size for most application is 2,048 bits. For equivalent security using ECC, key size of only 224 bits is needed. The difference becomes more and more pronounced as security levels increase and as hardware gets faster, and the recommended key size must be increased. A 384 bit ECC key matches a 7860-bit RSA key for security. The proposed protocol inherits the security and implementation properties of the elliptic curve cryptosystems which seem to offer the highest cryptographic strength per bit among all existing public key crypto systems. Thus the use of ECC in wireless communication is highly recommended.

REFERENCES

[1] William Stallings, Cryptography and Network Security, Pearson Prentice Hall

[2] An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication, 2nd International Workshop on Discrete Algorithms and methods for Mobile Computing and Communications, Oregon State University, October 30, 1998,

[3] Dr. Kevin Anderson, MWSU, Elliptic Curve Cryptography, andersk@missouriwestern.edu,

[4] Nancy Cam-Winget, Russ Housley, Security Flaws in 802.11 Data Link Protocols, Communications of the ACM, vol. 46. No. 5, May 2003.