Development of security scheme on wireless sensor network based on Elliptic Curve Cryptography

Dongmei Li[1, a], Yan Liu[2]

[1]Nanyang Institute of Technology, Henan Nanyang, 473004, China

[2]Information Engineering Institute, Zhongzhou University, Henan Zhengzhou, 450044, China

[a]lidongmeiedu@163.com

Keywords: Elliptic Curve; Wireless sensor network; Cryptography; Security; Public key cryptosystem

Abstract. Wireless sensor network may encounter eavesdropping, message modification, message injection, route spoofing, denial of service, malicious code threats. This paper discusses the application of Elliptic Curve Cryptography in security in wireless sensor networks, discusses a wireless authentication and key agreement protocol based on elliptic curve cryptosystem. The paper proposes development of security scheme on wireless sensor network based on Elliptic Curve Cryptography. Safety examples prove that the proposed algorithm of wireless sensor network is effective.

1. Introduction

With the continuous development of information industry and the extensive use of mobile Internet, mobile phones and other mobile devices can provide more diverse services, and gradually become an integral part of daily life, but its safety has become increasingly prominent. How to effectively protect mobile phone users' personal information and data security, and it is as the current social issues of common concern. Cryptography as the core areas of information security technology provides a variety of cryptographic algorithms and application protocols to meet the needs of practical application.

Wireless sensor network security demand is mainly manifested in the following aspects: confidentiality is to ensure that the communication between sensor nodes in wireless sensor network integrity is to malicious nodes provide convenient data loss or damage to attack [1]. Integrity network node receives data a packet in the transmission process is not inserting, delete, and modify, to ensure that the received message and the source message are completely consistent.

Wireless sensor networks need to achieve some of the most basic security: confidentiality, point-to-point message authentication, integrity, authentication, freshness, broadcast authentication and security management. In addition, in order to ensure that the data fusion of data source information retention, watermarking technology has become the research contents of security in wireless sensor networks. Although the security of wireless sensor network, without introducing too much content, but the characteristics of wireless sensor network decides the safety and the traditional network security it in a very different research methods and calculation methods.

Elliptic Curve Cryptography Compared with other public-key cryptosystem. Studies have shown that for elliptic curve cryptography 160bi long has the security key with RSA or DSA keys in the 1024 bit long has the very security. And, in a finite field, there can be a lot of elliptic curve cryptography for the establishment [2]. This paper focuses on Elliptic Curve Cryptography Research and implementation of this project to start in elliptic curve cryptography for existing in-depth study, based on the design and implementation of a safe and efficient elliptic curve cryptosystem.

Distributed key management and hierarchical key management according to the network structure, WSN key management can be divided into distributed key management and hierarchical key management two. Negotiation, node key update is accomplished by using node pre distribution key and mutual cooperation. In the hierarchy of WSN key management, the nodes are divided into several clusters, each cluster has a cluster head strong (cluster head) to take charge of the management of it.

2. Elliptic Curve Cryptography

MOV-based domain reduction method only when the degree of expansion of the definition is appropriate for a small time is embedded is valid. Then baby-step giant-step algorithm's time complexity is # E (Ep) a function of the time index algorithm by # E (Ep) determined parameters.

In the elliptic curve E is on exactly one point [3]. Called the infinity point. Namely (0: I: 0) with 0.

Non-homogeneous coordinates can be expressed in the form of Weierstrass elliptic curve equation: Let x = X / Z, y = Y / Z. So the original equation into: equation1.

y2+a1 xy+a3Y=X3+a2X2+a4x+a6 (1)

The E algorithm ⊕ has the following properties:

If the line L cross E at point P, Q, R (not necessarily different), then

(1)(P ⊕ Q) ⊕ R = O.

(2)For any P ∈ E, P ⊕ O = P.

(3)For any P, Q ∈ E, P ⊕ Q = Q ⊕ P.

(4)Let P ∈ E, there is a point, denoted by - P,

so P ⊕-P = O.

For any P, Q, R ∈ E, a (P ⊕ Q) ⊕ R = P ⊕ (Q ⊕ R) That is to say, E constitute a rule ⊕ for computing the exchange group. Further, if E is defined in K, then E(K):={(x,y)|y2+a1xy+a3y=x3+a2x2+a4x+a6} ∪{o} is a subgroup of E. Now we give the exact formula for computing group [4].

Let the general Weierstrass elliptic curve equation E: E:={(x,y)|y2+a1xy+a3y=x3+a2x2+a4x+a6} ∪{o}. Let P1=(x1,y1),p2=(x2,y2) are two points on the curve E, then-P1=(x1,-y1-a1x-a3), as is shown by equation2.

$$\begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} & X_1 \neq X_2 \\ \lambda = \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & X_1 = X_2 \end{cases} \qquad (2)$$

The following shows the use of SEA algorithm to select a large prime field elliptic curve on security steps. Select a large prime number field of secure elliptic curves.

Input: a finite field of size q;

Output: the elliptic curve E (a, b), # E (a, b) = nh, n is a large prime factor, n> 2160 and n> 4q.

(1)Random GF (p) on an elliptic curve E (a, b):

(2)The SEA algorithm to calculate the # E (a, b);

(3)The use of large integer factorization algorithm decomposition # E (a, b), and detection of # E (a, b) whether the decomposition in> 2160 the prime factor n. If not, go back to (1).

Wireless sensor network may encounter eavesdropping, message modification, message injection, route spoofing, denial of service, malicious code threats. In addition, in wireless sensor networks, the concept of security has also changed, the communication security is one of the important part, privacy protection becomes more and more important, and authorized the importance of reduced.

Each based on elliptic curve public key cryptosystem operations, are included by some elliptic curve domain parameters defined on the finite field arithmetic on elliptic curves. Work in SEC1 the ECC draft, as defined by the elliptic curve domain parameters consisting of a six even.

T = (p, a, b, G, n, h) (3)

Where: integer p is a finite field Fp; two elements a，b∈Fp specified by the definition of an elliptic curve; G represents a point; n is prime and equal to the point G of order; h=#E(Fp)/n, is called the cofactor.

As the elliptic curve cryptosystem security only with the security of elliptic curve, and therefore, we can select for the establishment of a class of elliptic curve cryptosystems secure in the establishment of such an elliptic curve cryptosystem can guarantee their safety. The security of elliptic curve is the difficulty of solving the ECDLP the decision, which through analysis of existing algorithms to solve a variety of ECDLP, accurately grasp the ECDLP problem solving for design and evaluation of the progress of fast and secure elliptic curve has very important significance. Security of elliptic curve that is resistant to attack a variety of algorithms has been attacks on elliptic curve.

3. For WSN to Achieve Elliptic Curve Cryptosystem

For example: elliptic curve equation E211 (1,1): y2 = x3 + x +1 elliptic curve point group of order 223, integer points on elliptic curves have 222. There is also a point at infinity 0. Take any point V (2,86), and then calculate the point of the elliptical cycle [5]. The basic idea is: use the law of addition operation described above, calculate the value of n nv = 0 is the point v of the cycle (stage). After a calculated n = 223. After verification of the above algorithm. That n = 223 is a prime number, so the point V can be seen as point G.

(1) The calculation of points on elliptic curves

① For each satisfy 0 ≤ x <p of X. Calculation of X3 + ax + b (mod p);

② For each of the previous step to get the results to determine if it has a square root of P mode. If not, in Ep (a,b) was not found in an x value of this point. If so, there are two square root operations to meet the y value (unless the value is a single y value of zero). These (x, y) value is Ep (a,b) in point.

(2) Points on the elliptic curve calculation cycle

1. Select the ellipse that q (x0, y0);

2. Calculate the q + q + ... + q, nq = 0 makes the establishment of minimum n, if y0 = 0, then. This point is no cycle;

3. Test whether n is prime, if not. Go back to step2.

The implementation scheme based on the elliptic curve encryption and digital signature, and it is first of all to parameters of elliptic curve domain to determine an elliptic curve. But not all are suitable for the elliptic curve encryption, Y2 X3 axes B is a class can be used to elliptic curve cryptography, is also the most simple. Below we select the Y2 X3 ax B as encryption curve us [6]. This curve is defined in the Fq: two satisfying the following conditions is less than P (P is a prime number) of non negative integers a, b: 4A3 27b2 0 (mod p) will meet the following equation (all points x, y), plus infinity ∞, form an elliptic curve.

A current attack of Elliptic Curve Cryptography Algorithms Elliptic curve cryptosystem depends on the security of elliptic curve is defined by the group on the difficulty of the discrete logarithm problem [7]. There are two solutions to the discrete logarithm problem of effective algorithms, namely Shank's baby-step giant-step algorithm and any cyclic group of index algorithms. Shank's baby-step giant-step algorithm is a basic group does not depend on the index algorithm, but it needs to group the order of the largest prime factor of safety index time is O(p), where n is the group F (Fp) order of the largest prime factor, expressed as # E (Fp)

Bob's decryption process: Bob receives Alice's ciphertext (36,189,136), the Executive

1. With the private key d = 112, calculate the point (x2, y2) = d (x1, y1) = 112 (36,189) = (94,129), calculated in Fp = 110.

2. By calculating m = C = 136 * 110 = 1 90, to recover the plaintext data m = 190.

The algorithm has been justified in the use of SEA the number of points after each test whether the selected curve of large prime factor, is a non-regular curve, whether the ultra-strange curve.

4. Application of Elliptic Curve Cryptography in Design Security Scheme for Wireless Sensor Network

At present in the elliptic curve point group is also no one can be found in exponential time algorithms for the solution of the discrete logarithm problem [8]. Therefore, in the premise of the same security people can be formed by elliptic curve order smaller point group set up password system. The amount of keys that the elliptic curve cryptosystem and it is save bandwidth, faster computation speed. These features make the elliptic curve cryptography is very suitable for computing speed and storage space is limited, such as smart card, radio equipment etc.

AIice send message m to Bob, Alice perform:

1. Find Bob's public key (E (Fp), G, n, Q);

2. The m expressed as a domain element m ∈ Fp, m will be expressed as 190;

3. In the interval [1, n-1] select a random number within the k, where select k = 57;

4. Calculated based on Bob's public key point x1, y1) = kG; (k a G addition) was (x1, y1) = 57 (2,86) = (36,189).

Taking full account of ECDLP attack algorithm and based on the analysis above, summed up select safe elliptic curve should follow some principles.

(1)SE selection of non-super singular elliptic curve, without selecting a singular elliptic curves, hyperelliptic curves, and anomalous elliptic curves;

(2)# E is not divisible by qk-1, 1 ≤ k ≤ 20.

Once the two sides have access to each other's public key, obtain information on both sides with his private key encryption [9]. Concrete is realized through its private key and public key by multiplying each other. In order to prevent the leakage of the certificate, the certificate is required to be delivered by encryption mode. In this protocol, the specific approach is: the server will generate a random integer g, then using the symmetric encryption algorithm to (RS, SX) and concatenated string certificate is valid for TS encryption, message encryption to the user end. The client decrypts the message, access to the server certificate and the random number G. The client then concatenated string has its own certificate and the certificate is valid for encryption, encrypted message to C1, and then sent to the server, as is shown by equation4.

$$x_3 = \begin{cases} \lambda^2 + \lambda + x_1 + x_2 + a & P \neq Q \\ \lambda^2 + \lambda + a & P = Q \end{cases} \tag{4}$$

Experiments show that, when the nodes in the network number, survivability of this scheme is better than the E-G scheme, but with the increasing number of compromised nodes, and it is the scheme becomes worse. Multiple key spaces of random key pre distribution scheme of Blom single key space scheme allows any network of two nodes can establish pairwise keys, and ensure that the compromised node number is less than the threshold value, the network will not disclose any confidential information. It will expand as the random key pre distribution scheme of multi key space.

Let P, Q are two points on E, L is the line through P and Q (over the tangent point P, if P = Q), R is L and E intersects the third point curve. Let L' is a straight line through R and Q, then P ⊕ Qis L' and E intersect the third point.

The session key agreement between km=Qk.x+g user end and the server end, is negotiated by both sides of communication [10]. The parameter Qk is obtained by the user and server's private key and the other's public key together, the private key only within the system based on ECDLP public key generation, transmission, also does not have the safe hidden trouble, at the same time generated by the server by sending a random number G is in encrypted form to the user terminal. Therefore, only the end user and server negotiation can calculate the session key, any one party alone can not calculate the session key, as is shown by equation5.

$$v = \begin{cases} \dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1} & P \neq Q \\ \dfrac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3} & P = Q \end{cases} \tag{5}$$

Elliptic curve cryptosystem has a maximum security, has been more and more widely used in the field of information security. To further improve the performance of elliptic curve cryptosystem and the application of elliptic curve cryptosystem based on specific environment are two main research direction of the elliptic curve cryptosystem. This paper mainly discusses the application of ECC system in the wireless network security, authentication and key agreement protocol is suitable for wireless network environment, and the function and security are analyzed and proved.

Summary

Elliptic curve cryptosystem is able to adapt to the future of communications technology and information security technology development of new cryptosystem, its anti-brute-force method is to use a large key space. The safety analysis also attracted national attention cryptologists and the relevant departments and attention, but research results are not great, maybe this can also be seen as elliptic curve cryptography has high strength evidence. The paper presents application of Elliptic Curve Cryptography in design security scheme for wireless sensor network. Therefore, most cryptographers of this cryptosystem are optimistic about the prospects. Currently, it has become a public key cryptosystem in research focus.

References

[1] Julio Lopez, Ricardo Dahab. An Overview of E1liptic Curve Cryptography, Technical report, Institute of Computing, State University of Campinas, Brazil, May 22， 2000, 11(2):183-192P

[2] Satoh T, Skjemaa B, Taguchi Y. Fast Computation of Canonical Lifts of Elliptic Curves and its Application to Point Counting, Finite Fields and Their Applications.2003, 9(1):89-101P

[3] Gebotys C. Design of Secure Cryptography Against the Threat of Power-Attacks in DSP-Embedded Processors. ACM Transactions on Embedded Computing Systems (TECS), 2004, 3(1): 92-113P.

[4] Bin Wang, Xiao Wang, Wangmei Guo, "A Secure Scheme with Precoding Approach in Wireless Sensor Networks", AISS, Vol. 5, No. 1, pp. 782 ~ 788, 2013

[5] Lutz, J., Hasan, A. High performance FPGA based elliptic curve cryptographic co-processor. IEEE Transactions on Information Technology: Coding and Computing, 2004, Vol.2, 486-492P

[6] K.Lauter, The advantages of elliptic curve cryptography for wireless security, IEEE Wireless Communication, 2004,11(1):64~67

[7] K.Fong, D.Hankerson,J.Lbpez etal. Field inversion and point halving revisited, IEEE Transactions on Computers, Aug. 2004,53(8):1047-1059P.

[8] D.Adachi and T. Hirata. Combination of mixed coordinates Strategy and direct computation for efficient Scalar multiplications, Communications Computers and signal Processing, PACRIM'2005:117-120P.

[9] Lasheng Yu, Nsoita Ivan, Li Jie, Linong Li, Renjie Liu, "Research and Implementation of an Effective Data Gathering Algorithm for Wireless Sensor Network", JCIT, Vol. 8, No. 4, pp. 98 ~ 107, 2013

[10] Zhang Li, Tong Xin, Threat Modeling and Countermeasures Study for the Internet of Things, *JCIT*, Vol. 8, No. 5, pp. 1163 ~ 1171, 2013.