The Design and Study of A Low Coupling Wireless Sensor Network Authentication Architecture

Jing He1, Chunlei Yin2, Yan Kang3,*

1 School of Computer Science and Engineering University of Electronic Science and Technology of China Chengdu, 611731, China
2 School of Architecture Engineering Yunnan Agricultural University Kunming Yunnan 650201, China
3 National Pilot School of Software, Yunnan University Kunming, 650091, China

Abstract — As wireless sensor networks become applied more and more widely, the existing security system certification structure hasn’t already met the needs of wireless sensor networks. In order to accommodate wireless sensor network to current application environment, people shall attach more importance on enhancing its securities and lowering communications cost calculation. On the grounds that its resources is limited and transport energy consumption is much larger than other communication network characteristics, we adopt a low coupling ECC algorithms and mutual authentication. In this paper, the author found that compared with traditional algorithms, low coupling ECC algorithm is optimized in doing the dot product, the remaining square determination as well as changing the key update. Hence the security strength of the same communication, the key length significantly reduced, while corresponding special space is relatively small, which means the capabilities fight against cyber-attack capabilities become stronger. In the same network, the improved ECC algorithm handles more encryption and decryption algorithm than conventional ECC algorithms does. Therefore, its safety has been effectively improved. Secure communication between the common node and cluster head node, potently prevents forgery and theft guarantee to inject malicious illegal information and transmit data through mutual authentication method.

Keywords - Wireless Sensor Network; Low Coupling ECC; Key Management; Two-Way Authentication

I. INTRODUCTION

In recent years, with the development of wireless technology, micro-electronics technology, embedded technology and sensor technology, wireless sensor networks (WSN) catches more attention in the field of information technology. Wireless sensor network (WSN), superior in self-organization, deployment, fast, high fault tolerance and concealment, such as technology, so it is suitable for the field goal, and physiological data acquisition, intelligent transportation systems, and uses its detection in many fields. At present, the wireless sensor network (WSN) is applied to the defenses forces, environmental science, the intelligent construction, medical, health, space exploration and high professional ...ACMZ was founded in 2005, a magazine (ACM transacted on sensor networks) published the research of wireless sensor network technology [1]. Announced in October 2006 that sensor network formation of branches of China computer Federation, the Agency as a non-commercial, cooperation between academic institutions, is a national platform for academic exchanges and cooperation, dedicated to attracting corporate participation, accelerating the industrialization process. In, the CITRIS of University of California in Los Angeles, Berkeley, MIT, IBM ASCENT of the University laboratory, crossbow technology companies, such as United States colleges and universities and well-known companies in the wireless sensor network technologies put forward effective solutions [2, 3]. Currently, Chinese Academy of Sciences, Software College of early stage of technology and industry chain of Wuxi industrial Institute, Computing of Shanghai Institute, Tsinghua University instrument science and Technology Institute wireless sensor network in the national completed in-depth research of theory and application in the long-term science and technology development planning platform for (2006-2 020 years)” will "sensor network and the intelligent information processing" for "focus field and priority theme" are in need of policy support. Wireless sensor network architecture has a great role in the formation of the industry [4, 5]. Townsend C put forward the basic random key pre-distribution scheme [6]. According to research presented by Branch J W, (LEACH) [7] is a low energy adaptive clustering hierarchy. At present, confidential information is massively transmitted in wireless sensor networks, thus its integrity and security of information transmission is facing great challenges. As the process of transferring information in the network node, no node authentication has closely link, so people cannot establish a mechanism of mutual trust between nodes. On account that current network traffic to the key length is too
long, only a short time is needed for network to decrypt, cannot guarantee the security of information. This thesis introduces a lot of networking and wireless monitor network application and key algorithm related to literatures calculated, according to the characteristics of its scope of application and work proposed improved low coupling ECC algorithm, to improve the wireless monitor network security communication and computation consumption.

II. STATE OF THE ART

A. Low Coupling ECC Algorithm

Compared with traditional algorithms, low coupling ECC algorithm is optimized in doing the dot product and the remaining square determination. Using the ECC algorithm for encryption and decryption, there will be a large number of dot product operations, such as:

\[ nP = P_1 + \ldots + P_n \]  

(1)

Optimization processes are as follows: At first, the n in the form of binary numbers, that is to say \( n = (n_1n_2\ldots n_{k-1}n_k) \). \( n_k = 0 \) or \( 1 \), \( k = \left\lceil \log_2 n \right\rceil + 1 \), followed by removing \( (n_1n_2\ldots n_{k-1}n_k) \) the most significant bit n, you can obtain \( (n_{k-1}n_{k-2}\ldots n_1) \). And finally, in accordance with the \( (n_{k-1}n_{k-2}\ldots n_1) \) in descending order, when \( n_k = 0 \), the calculation \( 2P \). When \( n_k = 1 \), the calculation \( 2P + P \), and calculates the initial value as a result of the next operation, that is to say \( 2P \Rightarrow P \) or \( 2P + P \Rightarrow P \).

Traditional ECC algorithm required \( n \) operations. After optimization strategy proposed in this paper [8], an average of only \( 3/2 \left\lceil \log_2 n \right\rceil \) times calculation, at most only \( 2 \left\lceil \log_2 n \right\rceil \) operations, thereby reducing the computation time and improve processing speed.

Suppose plaintext \( m \) mapping curve \( P \), and the following relationship:

\[ 256m \leq x \leq 256(m+1) \]

(2)

\[ P_m(x, y) \in F_p \]

Improved algorithm proposed as follows:

First of all, remaining square of the decision variable is identified as J, and satisfies the condition \( J = 1 \); followed by suppose A is even, then it can be decomposed into:

\[ \frac{A}{P} = \frac{2}{P}((A/2)/P) \]

(3)

After \( 2/P \) is solved substituted into (4):

\[ J(2/P)\Rightarrow J, A/2 \Rightarrow A \]

(4)

Suppose A is an odd number, then it can be decomposed, the following formula:

\[ \frac{A}{P}\frac{P}{A} = \frac{A}{P}((P \mod A)/P) \]

\[ = (-1)^{(l(A-1)/2)((P-1)/2)} \]

(5)

\[ (A/P) = (-1)^{(l(A-1)/2)((P-1)/2)}((P \mod A)/P) \]

(6)

If the calculation result is a portion 1, then return to step two, and vice versa jump algorithm.

In this paper, the user's private key constantly changing, in order to ensure the security of the private key of the user to register and obtain PK save the corresponding user's private key SK. The effective time of the public key into T time periods, were recorded as 1, 2, ..., T. In the period of time public key is 1, the user's private key \( SK_1 \), public key period 2, the user private key \( SK_2 \), and so on. The use of one-way hash function \( SK_{t-1} \) to \( SK_t \) transform operation, when the \( SK_t \) transformation success. Immediately remove \( SK_{t-1} \), and convert the update process is as follows:

\[ T_1 T_2 T_3 \ldots T \]

(7)

Because the whole optimization process is the use of a one-way hash function which transforms its operation, it has greatly increased from the front after a private projection of difficulty, improving the security of information.

B. Mutual Authentication and Key Agreement Protocol

This system is used in two-way authentication protocol between devices A and B. The device A is data transmitting side, and the device B is used for data receiver. A representative of the device's public key PKA, PKB B represents the device's public key [9]. Mutual authentication protocol herein include: the exchange of certificates, key negotiation and challenge-response mechanism. Protocol Authentication distance is shown below:

![Figure 1. Mutual authentication protocol flowchart](image)

III. METHODOLOGY

Before deployment, password management center selected hash function, elliptic curve parameter information, DOI 10.5013/IJSSST.a.16.5A.07 7.2 ISSN: 1473-804x online, 1473-8031 print
public / private key matrix and other information, password management center node identification, generation and distribution of key parameters and each node certificates, so that each node has its own identity, such as divided key, private key combinations, the combination of public-key matrix, certificates, and elliptic curve parameters and other information. System work firstly generates the key pair system and a communication group key, and finally establishes ordinary nodes and other nodes of mutual authentication and key agreement [10].

In wireless sensor networks, only legitimate key combinations of nodes may vary. Depending on each other’s identity and split key, other combinations of public key (CPK) are calculated, there is no third party involved in the certification process can be simple to achieve. CPK-based ECC system may be a small number of public / private key matrix having a large public / private key pair combined, nodes only need to store a small matrix, can achieve a lot of network security authentication node. CPK-based ECC system may be a small number of public / private key matrices, combined with large-scale public / private key pair, the node only needs to store a small matrix to achieve a lot of network security authentication node.

IV. RESULT ANALYSIS AND DISCUSSION

A. Computation Overhead

In the node and re certification process, repetitive use of the certification of the encryption and decryption and the scalar multiplication of digital signature algorithm, are the main computational overhead. Montgomery type light fast point multiplication based on computational complexity is low, and other algorithms are as follow (Table 1, M denotes multiplication, S denotes square, I denotes inverse, n denotes the scalar multiplication in D binary digit).

<table>
<thead>
<tr>
<th>Plan</th>
<th>Computational complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>K.Okeya and K.Sakurai’s plan</td>
<td>49M+12S+2I</td>
</tr>
<tr>
<td>Y.Futa and M.Ohmori’s plan</td>
<td>(n-53/18)(4M+2S)</td>
</tr>
<tr>
<td>Ladue’s plan</td>
<td>3I+(13.875n+30.25)M+(9.25n+2.5)S)</td>
</tr>
<tr>
<td>Text scheme</td>
<td>(6d</td>
</tr>
</tbody>
</table>

Through the algorithm computational complexity analysis and calculation, the most time-consuming point multiplication algorithms significantly reduced, namely in the negotiation process of the key algorithm, the dot product operation is only 11 operations, and other time-consuming more certification computation is only 2 times.

B. Memory Overhead

At the same security strength, the smaller the key length algorithm is, the safer it is. Based on the same network in the traditional ECC algorithm and the improved ECC algorithms safety performance test results are as shown below:

![Figure 3. Comparison of node connectivity](image)

As it can be seen from the figure, after the first anti-cyber-attack, improved ECC algorithm performance in this paper is better than the unmodified ones. And in the same security strength, the improved algorithm ECC key sizes smaller, indicating that the occupied space is small, which means the anti-cyber-attack ability.

V. CONCLUSION

Working for wireless sensor network security has higher requirements. In order to enhance the security of communications, the system uses a low coupling ECC algorithm and two-way authentication technology, ECC algorithm not only saves storage space but also increase the key. The key is to break the required time. Two-way authentication technology enables network attacker to intercept the correct certificate private key even legitimate users cannot get, hence anti-attack ability is improved. This system increases the overall communication process safety and reliability, creating access to the network and network attacker who cannot steal information, hence reduces the probability of packet loss.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (61363021); Science Research Fund of Yunnan Provincial Education Department (2014Y013).

REFERENCES

detection in wireless sensor networks”, Knowledge and information

clustering and ant colony optimization for wireless sensor networks”,

wireless sensor networks in smart grid”, Industrial Electronics, IEEE

in wireless sensor networks: A survey”, Communications Surveys &

Philosophical Transactions of the Royal Society A:Mathematical”,

no. 10, pp. 92-95, 2008.

vol. 20, no. 9, pp.15-21, 2005.


wireless sensor networks with unreliable links”, Computers, IEEE