A Node Authentication Protocol based on ECC in WSN

Qing Chang
School of computer science and technology
China University of Mining and Technology, CUMT
Xuzhou 221116, China
cschangqing@163.com

Yong-ping ZHANG, Lin-lin Qin
School of computer science and technology
China University of Mining and Technology, CUMT
Xuzhou 221116, China
ypzhang@cumt.edu.cn

***Abstract*—This paper improves an authentication protocol based on The Elliptic curve Cryptography, and applies it to WSNs. This scheme contains system initialization, node registration and authentication phase. It continues to use the primary scheme's high efficient multiplication operation method, and the sensor node store the other ID's hash value as the premise of the authentication. Besides, this scheme increases an authentication phase between sensor nodes using The XKAS Key Agreement Scheme. Conclusion shows that the improved agreement has lower consumption for wireless sensor network.**

Keywords—Elliptic Curve Cryptography; Authentication; Wireless sensor network; XKAS

I. PREFACE

With the development of the low-power consumption wireless communication technology, micro-sensor technology and integrated circuits technology, wireless sensor network (WSN) has been growing strong. And it has been widely used in military, agriculture, environmental monitoring, health care, building monitoring, space exploration and other special fields.

As the core and important basic link of the security mechanism, authentication has always been a hot area of security research on wsn. Because of the sensor node's limited energy, communication and storage resources, the authentication protocol in the traditional network must be improved to apply to WSN.

Using symmetric encryption to authenticate needs to carry large amount of pre-distribution key, and the node will consume too large memory space. So, using this authentication method in the large-scale WSN will make the network expandability very bad. Public Key Cryptography (PKC) has the unique authentication reliability and can prevent the Man-In-The-Middle Attack [1] effectively. Many scholars studied on the public key arithmetic in WSN. Such as TinyPK [2] entity authentication protocol which based on low-level RSA [3] proposed by R.Watro, and strong user authentication protocol [4] proposed by Z.Benenson et al.

Compared with RSA and other public-key cryptosystem, elliptic curve cryptography (ECC) has many special advantages such as lower requirements of the bits length of key, higher intensity, less parameters, which is especially for space constrained and bandwidth constrained situation [5]. So, ECC is more compatible to be used in the WSNs which have limited resources [6].

Table 1 [7] shows the key length of three cryptography under the same security property, as follows:

TABLE I. THE KEY LENGTH RATIO BETWEEN ECC, RSA AND DSA

Key length of RSA/DSA	Key length of ECC	Key length ratio of RSA/ECC
512	106	5：1
768	132	6：1
1024	160	7：1
2048	210	10：1

About authentication on WSN, this article improved an authentication protocol based on elliptic curve, using high-efficiency operation method [8], less node storage and computation, which is applicable to wireless sensor network.

II. BACKGROUND KNOWLEDGE

A. Wireless Sensor Network

The traditional computer network is generally to meet the various needs, but WSN is usually for the data-centric information-gathering work for a specific demand [9].

Sensor network usually contains sensor node, the sink node and the base station (BS). A large number of sensor nodes are deployed in or near the surveyed area randomly, and constitute the network by self-organization. Sensor node detects data and transmits it to the other node hop-by-hop. The transmission may be proceeded through one or more nodes, and arrive at the sink node after multi-hop, then reach BS finally. Users deploy and manage sensor node, publish testing task and collect test data through BS. The WSN architecture in this article is shown in Fig.1. BS is the base station, sensor nodes can communicate with BS directly.

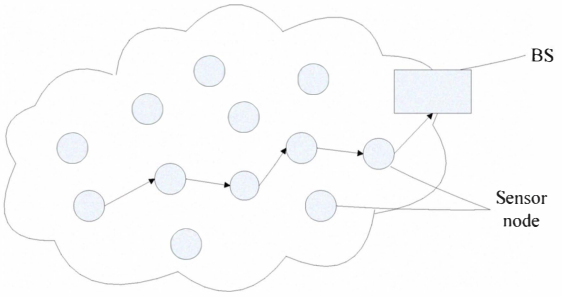

Figure 1. Wireless sensor network architecture

Assume that BS is safe, and each sensor node has its own unique identity. Sensor node can authenticate and communicate with each other, and can communicate with BS also. BS can communicate with a sensor node through the secure channel, and can broadcast messages. After deployed in the work area, the sensor node must be authenticate with its neighboring nodes and BS mutually [10], and this provides the security access mechanism for all the nodes to access the self-organizing.

B. Elliptic Curve Cryptography(ECC)

Elliptic curve E defined on the domain F can be defined by the following Weierstrass equation (1):

$$E: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \quad (1)$$

Where $a_1, a_2, a_3, a_4, a_6 \in F$ and $\triangle \neq 0$, $\triangle$ is the discriminant of E. F is a domain. If number (x, y) can satisfy the above equation, then it can be called the point of the elliptic curve E defined on domain F. Domain F can be the field of rational number, the complex number and finite field. This article studied the elliptic curve defined on prime fields F_q, and the elliptic curve E is constituted by point (x, y) and the point at infinity which satisfy equation $y^2=x^3+ax+b$, where $x, y, a, b \in F_q$, $F_q=\{0, 1, 2, q-1\}$.

ECC is a kind of cryptography obtained by the elliptic curve finite group on finite field insteading of the finite group on over the cryptography based on the discrete logarithm problem. It is built on the Abelian group which composed by the points of the elliptic curve on finite field F_q. The security of ECC is based on the difficulty of solving the elliptic curve cryptography disperse logarithm problem (ECDLP) [11]. Description of ECDLP: given a finite field F_q and a elliptic curve E defined on F_q, and we know the base point P, the order n and a point Q, where $Q \in \langle P \rangle$. When we choose a number k, it is easy to compute $Q=kP$ (kp is called ECC point multiplication), but in reverse, when Q and P are known, compute $k=log_pQ$ is very hard. Choosing a set of properly elliptic curve parameters, ECDLP will be a difficulty problem for current calculation level.

III. THE AUTHENTICATION SCHEME BASED ON ECC

This article improved the authentication system designed in [8], it based on XKAS Key Agreement Scheme for the WSNs. After system initialization, BS distributes keys for each node, and nodes do mutual authentication and communication. The process of the agreement is shown as follows.

1) System Initialization

Using the elliptic curve method to generate mentioned in [8], this system (BS) generated a safety elliptic curve. Its base parameters can be defined as follows:

$$Params=\{F_q, E, G, n, H, s, P_s\}$$

Where F_q the prime field of the elliptic curve, E is the elliptic curve, G is the base point of the elliptic curve, n is the order of G and be a prime number, and H is a one-way mapping function which can map any string to domain F_q. $s \in F_q$ is the system private key which selected by itself. $P_s=sG$ is the system public key. System private key stored by the system itself, its public key and other parameters published.

2) Registration

Each sensor node has a unique identity ID of the network, which stored by the sensor node itself. At this phase, nodes register for their identity at BS. Any node whose ID is in the prestore ID table is legal node.

Node a select a random number $s_a \in F_q$ as its private key, and compute $P_a=s_a^{-1}G$ as its public key, then transmit ID_a and P_a to BS.

BS compute $H(ID_a)$ and $R_a=sH(ID_a)$, then transmit R_a to sensor node a through the secure channel, and broadcast $H(ID_a)$ and P_s. The other nodes store $H(ID_a)$ and P_s.

Node a verify $s_aR_aP_a=P_s\ H(ID_a)$. If the equation is right, then registration is successful. Where both R_a and P_s have the signature of BS, so the attacker can't forge.

3) Authentication

Node A and B must be authenticate mutually before communication. Now we assume that they have determined their public and private keys. After BS broadcasted the hash value of a node ID, other nodes store the hash value. Instead of storing node ID, it decreases the node storage content.

When node A requests for B's certification, node B is first to see if it has node the ID hash value of A. If it has, then begin to authenticate. If not, then refuse authentication. Authentication steps were shown in Fig.2.

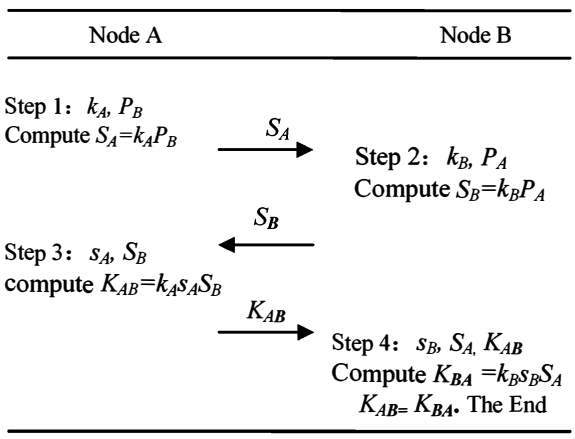

Figure 2. Authentication protocol between two sensor nodes

Step 1: Node A selects a random number k_A and gets B's public key P_B from BS, then computes $S_A=k_AP_B$ and sends it to node B.

Step 2: Node B selects a random number k_B, and gets A's public key P_A from BS, then computes $S_B=kB_AP_A$ and sends it to node A.

Step 3: After got S_B from B, A computes $K_{AB}=k_As_AS_B$ using its private key s_A, then sends K_{AB} to B.

Step 4: After got S_A from A, B computes $K_{BA}=k_Bs_BS_A$ using its private key s_B, then compares K_{AB} with K_{BA} to accomplish the authentication.

Verification process is shown as follows:

$$K_{BA}=k_B s_B S_A=k_B s_B(k_A P_B)=k_B k_A s_B P_B=k_A k_B G$$

$$K_{AB}=k_A s_A S_B=k_A s_A(k_B P_A)=k_A k_B s_A P_A=k_A k_B G$$

IV. ANALYSIS OF THE PROTOCOL

Security and efficiency is a pair of contradiction. When we asking for stronger security, there will always make the lower efficiency of the program; and at the time when we looking for high efficiency, the security always cannot be guaranteed. Thus, it's very important and necessary to seek a balance between the two in an agreement. This article analysis the agreement from the aspects of security and efficiency.

A. Security

This scheme accomplished the authentication between nodes based on the security of XKAS Key Agreement Scheme.

(1) Node's private key is stored by itself, it can't be revealed even BS is under attack. Based on the difficulty of solving ECDLP, even if the attacker got node's public key, he can't get its private key. And the private key is a random number selected by node itself, when the private key is untrusted, the node can reselect a random number for private key and register in system.

(2) In authentication process, the attacker can get k_A and k_B by cracking the private key or intercepting S_A and S_B for attacking. But the above problems are all based on the difficulty of solving ECDLP, the attacker can not attack by the above way. So, this scheme can resist passive attack.

(3) Now that the attacker cannot get node's private key, even if S_A and S_B are falsified in communication process, the attacker cannot disguise himself as one side to accomplish authentication with the other side. So, this scheme can resist active attack.

(4) The node needs to check the other's ID hash value before authentication. Because the node's ID is the unique one which cannot be forged, this scheme can resist man-in-the-middle attack.

(5) In authentication phase, this scheme uses the random number to accomplish authentication, so it can resist replay attack.

(6) Hash function is a kind of one-way irreversible function, so any attacker cannot decrypt it. And nodes store the ID hash value which can conceal the node's real identity.

B. Efficiency

In this authentication system, ECC multiplication is the primary operation mode, so its efficiency directly determines the performance of the system. Therefore, it can effectively enhance the performance of the system to use the fast algorithm for ECC multiplication and less multiplication number.

In this protocol, ECC multiplication operation consumes the most amounts. From the whole program, ECC multiplication times in various stages are shown in Table 2.

TABLE II. NODE MULTIPLICATION TIMES

Node / Stages	Node A	Node B
System Initialization	0	0
Registration	1	1
Authentication	2	2
Total times	3	3

In this scheme, sensor node only stores the other node' s ID hash value which decreases the consumption of the node memory space, and provides the condition for the expansibility of the network. Considering the limited sensor node traffic, the node traffic is 3 times in the communication process designed in this scheme. Compare with the primary scheme, this protocol leave out the tedious calculation for public and private keys, which makes the scheme simpler. And without additional digital signature, this scheme avoids additional communication overhead. Based on the low consumption of node storage and communication traffic and the high efficiency ECC multiplication algorithm, the 3 times node multiplication in this scheme is more reasonable.

V. CONCLUSION

Based on the principle of XKAS Key Agreement Scheme, this article increased a node authentication stage on the basis of the improving of [8]. This scheme is consisted of system initialization stage, node registration stage and node authentication stage. In the improved system initialization and node registration stage, the tedious calculation for public and private key was omitted, so that the public and private keys are easy to update and more secure. The authentication stage based on XKAS key agreement scheme can resist passive attacks, active attacks, man-in-the-middle attacks and replay attacks. This scheme is simple in design. Nodes store the ID hash value instead of the node ID to reduce the consumption of the node storage. And this scheme adopted the efficient ECC multiplication operation method and small number of communication and operation, which makes the calculation, storage and communication costs are lower.

REFERENCES

[1] Yi Jiang, Haoshan Shi. Cluster-Based Strategies for Public Key Authentication in Wireless Sensor Networks[J]. Chinese Journal of Sensors and Actuators, vol 20, no.6, 2007.

[2] WATRO R,et al. TinyPK:secuting sensor networks with public key technology. Proceedings of the 2nd ACM Workshop on Secutity of Ad hoc and Sensor Networks[C]. New York, 2005. 135-142.

[3] D Boneh, H Shacham . Fast Variants of RSA[C]. RSA Laboratories'Cryptobytes, 2002, 5(1): 1-8.

[4] Zinaida Benenson, Nils Gedicke, Ossi Raivio. Realizing Robust User Authentication in Sensor Networks [C]. Workshop on Real-World Wireless Sensor Networks (REALWSN) , 2005. 135-142.

[5] Youan Xiao. The Study of Elliptic Curve Cryptography System[M]. Huazhong University of Science and Technology press,2006:140-144.

[6] Limin Sun,Jianzhong Li,Yu Chen. Wireless Sensor Network[M]. Tsinghua University Press, 2005.

[7] WANG Wei-hong, LIN Yu-bing, CHEN Tie-ming. The Study and Application of Elliptic Curve Cryptography Library on Wireless Sensor Network. 2008 11th IEEE International Conference on Communication Technology Proceedings[C].

[8] Huaping Xiang,Zhongbao Wan. Design and Implementation of Identity Authentication System Based on ECC[J]. Control & Automation, vol 23, no.1-3, 2007.

[9] Jie Yang,Hui Li,Xiaoyuan Li. Wireless Sensor Networks Based on the WAPI Authentication[J]. Electronics Technology. no.4, 2006.

[10] WONG, et al. A dynamic user authentication scheme for wireless sensornetworks. Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference[C]. 2006: 244-251.

[11] Darrel Hankerson,Alfred Menezes, Scott Vanstone.Guide to Elliptic Curve Cryptography[M]. Publishing House of Electronics Industry, 2005:147.