Xiaorong Cheng[1], Mingxuan Li[2]

North China Electric Power University.BaoDing, China (1,2)

The authentication of the grid monitoring system for wireless sensor networks

Abstract. *With the extensive application of wireless sensor networks, security issues get more and more attention. So this paper designs a authentication program based on elliptic curve cryptosystem，that is applied to distribute network monitoring system for wireless sensor networks. According to mathematical principles and methods in elliptic curve cryptosystem, designs specific implementation process of authentication program. Finally, we analyze the practicality and effectiveness of this program in the respects of communication overhead, computational and safety.*

Streszczenie. *W artykule przedstawiono program weryfikacji użytkownika w sieci czujników bezprzewodowych, oparty na kryptografii krzywych eliptycznych. Algorytm dokonuje implementacji systemu weryfikacyjnego. Dokonana została analiza praktyczności i efektywności systemu.* ***(System weryfikacji w systemie monitoringu sieci czujników bezprzewodowych).***

Keywords: wireless sensor network; elliptic curve; authentication.
Słowa kluczowe: sieć czujników bezprzewodowych, krzywa eliptyczna, weryfikacja.

Introduction

With more and more intelligent power grid, distribution network monitoring system, a variety of wireless sensor real-time acquisition and processing nodes within the coverage area of various parameters. These sensors can be used to monitor the electrical equipment, the node is installed on the device, temperature and humidity sensors, pressure sensors, current and voltage sensors, different monitoring information to understand the running status of devices, monitor the use of equipment management[1].

However, wireless sensor networks are often deployed in open outdoor or no man's land, and are vulnerable to attack or sabotage, such as Sybil attack, denial of service attacks, wormhole attack, Hello flood attack[2]. It is necessary to eliminate the security threats in information transmission through the authentication method. Network, the energy of some nodes are quickly exhausted or has run out ,then exit the network. The nodes must be authenticated before communicate with each other, in order to avoid an attacker to use these exit network nodes to impersonate and forged node; in addition, if some of the active nodes is captured by the attacker, the ID of these nodes must also be broadcast to the whole network, and removed from the legal list. Therefore, authentication is very important. in connection with the grid monitoring system for wireless sensor networks[2,3].

Authentication thinking

The authentication includes between the cluster head and cluster nodes and cluster head and cluster head. The clustering stage within the cluster, firstly we determine the cluster head, if the node N_i ask to join in the cluster , $S_b \neq S_b'$ is the cluster head , N_i to CH_j initiate the request,in order to prevent the attacker node from counterfeit identity, then must carry on the two-way authentication between cluster heads and ordinary nodes; between the clusters, and sometimes a cluster head is far from the base station, it sends message to the base station, that must need forward of data packets with the other cluster head, now the communication between cluster head and cluster head needs to be authenticated. The authentication between cluster nodes and cluster head belongs to the many-to-one communication mode ,the cluster head and cluster head belongs to the one-to-one way, in order to save computation and communication overhead, in connection with the two different certification programs,we designs the two different programs.

In the view of authentication function, the role and relationship of each part of the sensor is described as follows:

Base station: it assigns the unique identity ID for all the sensor nodes in the entire network, and issues public and private key pairs for each node in the initialization process of the whole network. Structure and function of base station ared shown in Figure 1.

Cluster head: They use the public and private key of nodes issued by the base station; when ordinary node apply to join in the cluster, through the base station completes the authentication between the cluster head.

Ordinary nodes: They use the public and private key of nodes issued by the base station to complete the authentication and session key negotiation.

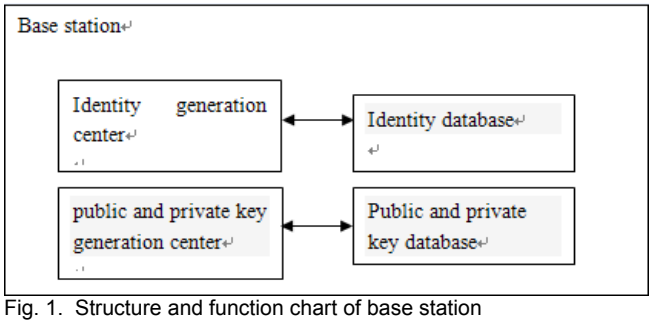

Fig. 1. Structure and function chart of base station

Table 1.Symbols and meanings

Symbolic name	meanings
Q_a	The public key of the node a
d_a	The private key of the node a
$S(a, d_a)$	Node a use the private key d_a to sign
$E(m, d_a, Q_b)$	The node encrypt proclaimed in writing m using the private key d_a and the recipient's public key Q_a
$hash(m)$	The one-way hash computation on the data m

Defined symbol and meaning, such as shown in Table 1.

(1)The configuration of the identity identifier

Before sensor are deployed in the network, the identity generation center of the base station configurate only the identity of a whole network ID number for each sensor node. The base station node identity database store the ID number of the identity of all nodes, to be used to query and

prevent generate duplicate ID numbers. If network cluster structure is changed, the base station needs compare the newly generated ID number with the existing data in the database ,in order to avoid the old identity identifier used again.

(2)The generateand issue of the public and private key of the node

In this article, the base station in the public and private key generation center based on elliptic curves generate public and private key stored in each node [4], described as follows:

Make p for a prime number , $F_p = \{0,1,2,\cdots,p-1\}$ is a finite field of mold p , the order of the domain is q , E is an elliptic curve, defined p in the finite field F_p , p is $E(F_p)$ the basis points, given the order of p is a prime number n , and p, E, q, P and n constitute a public parameter group. The private key is randomly selected positive integer d in the range $[1, n-1]$, the corresponding public key is $Q = dP$.

The public and private key of the node is the core of the security certification, and its security depends on the elliptic curve discrete logarithm problem.

Authentication process

Initialization

During initialization, it only set the identity of the whole network ID for each node ,in the offline environment, the base station assign an elliptic curve for each node in the network, and according to the elliptic curve cryptography mechanisms, randomly allocate the public and private keys for each node. Base station saves all the ID number of each node and the corresponding public key and private key. Cluster head saves the public key of the base station, and put the public key of the next hop cluster head into the memory. Nodes release the public key , and each node save their own private key.

Select an elliptic curve $E(F_q)$ to determine a basis point p , the order of p is n, and establish the key pair (d, Q) ,where d is the private key, $Q = dP$, Q is the public key.

(1)The base station storage elliptic curve $E(F_q)$, a one-way hash function $H(x)$, the public key Q_{bs} , the private key d_{bs} , and each node's public key and private key.

(2)The cluster head CH_j storage elliptic curve $E(F_q)$, a one-way hash function $H(x)$, the public key of the base station Q_{bs} , public key Q_{CH_j} and private key d_{CH_j} based on elliptic curve mechanisms, and public key of the next hop cluster head.

(3)Ordinary nodes in the cluster N_i storage oval curve $E(F_q)$, a one-way hash function $H(x)$, and public key Q_i and private key d_i based on elliptic curve mechanisms.

The certification between cluster head and nodes in the cluster

(1)The certification process

The cluster head broadcast messages to invite around the node joining in the cluster ,the messages contain its own public key.

Ordinary node N_i requests to join a cluster ,which CH_j is in ,where using the private key sign, in order to prove their legal status.

(1) $N_i \to CH_j$: $N_i \| S(N_i, d_{n_i})\ \alpha + \beta = \chi$.

where: N_i –the node ID number.

CH_j received packets of N_i , not N_i certification, and the packets, that N_i sent, together with the own ID and the ID of N_i is encrypted with the private key ,then sent to the base station.

(2) $CH_j \to BS : CH_j \| E(CH_j \| N_i \| S(N_i, d_{n_i}), d_{ch_j}, Q_{bs})$

Since the base station save the public and private key of each node ,it can decrypt the message which is sent by CH_j , and then verify the signature of N_i . If authentication is successful, generate the key K_{ch_j, n_i} of the cluster head nodes and ordinary nodes in the cluster, and use their private key to encrypte the newly generated keys, and finally send $BS \| E(K_{ch_j, n_i} \| Q_{n_i}, d_{bs})$ to CH_j . If the validation fails, then inform the entire network N_i is the illegal node.

(3) $BS \to CH_j : BS \| E(K_{ch_j, n_i} \| Q_{n_i}, d_{bs}, Q_{ch_j})$

CH_j received the BS response information, use its own private key d_{ch_j} to decrypt , get K_{ch_j, n_i} and Q_{n_i} ,and then d_{ch_j} encrypt $CH_j \| N_i \| E(CH_j \| K_{ch_j, n_i}, d_{ch_i}, Q_{n_i})$ send to N_i . Once the cluster head received the BS return message, look N_i after CH_j , can determine the cluster nodes N_i as a legitimate node.

(4) $CH_j \to N_i : CH_j \| N_i \| E(CH_j \| K_{ch_j, n_i}, d_{ch_i}, Q_{n_i})$

N_i Receipt the packets by CH_j senting, with their own private key d_{n_i} to decrypt ,to verify the identity of nodes CH_j ,and get the key K_{ch_j, n_i} communicated with the cluster head. At this point, the legitimacy of the cluster head node is completed by the common node in the cluster. CH_j and N_i establish a communication key K_{ch_j, n_i} , and then N_i and CH_j can use this key for security communications based on symmetric key.

(2)Program analysis

Communication overhead: In many certification programs, each sensor node communicate with nodes around it in exchange for the key ,and lead to the very large communication overhead. The proposed program between the nodes in the cluster does not require any communication, simply communicate with the cluster head, which cluster the node is in, then can complete the certification and establish the communication key, the communication overhead is small, reducing the energy consumption of nodes, thus extending the network lifetime.

Computational overhead: Considering that the calculation throughout the network in the certification between the cluster head node and ordinary nodes as well as negotiating session keys. The cluster node N_i distribute

the encrypted identity to the cluster head node CH_j, CH_j sent the received packet encrypted to the base station. When authentication is successful, the base station generates the call key to send to the cluster head CH_j, the cluster head decrypt and then send their own identity and the encrypted call key to to thecluster nodes N_i.

Security: In the certification process, the discrete logarithm problem based on elliptic curve cryptography mechanism, the attacker intercepted the message is in no way to crack the key through the message, each step in the transmission of information need the recipient's private key to unlock, so this certification process has higher security.

Authentication between cluster head and cluster head

(1)The authentication process

Suppose that two cluster heads CH_a and CH_b need data forwarding, then need for mutual authentication before communicate.The use of elliptic curve cryptography mechanisms, authentication process is as follows:

CH_a :Select a random number $r_1 \in [1, n-1]$, calculate $T_a = r_1 P$, then T_a will be passed to CH_b.

(5) $CH_a \rightarrow CH_b : CH_a \| T_a$

CH_b :Select $r_2 \in [1, n-1]$, calculate $T_b = r_2 P$, $S_b = d_b T_a$, $S_a = r_2 Q_a$.

(6) $CH_b \rightarrow CH_a : T_b \| CH_b \| hash(CH_b \| S_b \| S_a)$

CH_a :Calculate $S_b = r_1 Q_b$, $S_a = d_a T_b$,then verify $hash(CH_b \| S_b \| S_a)$,then

(7) $CH_a \rightarrow CH_b : hash(CH_a \| S_b \| S_a)$,

Equation verification process as follows:

(8) $CH_a : S_b = r_1 Q_b = r_1 d_b P = r_1 P d_b = T_a d_b = S_b : CH_b$

(9) $CH_a : S_a = d_a T_b = d_a r_2 P = d_a \Pr_2 = Q_a r_2 = r_2 Q_a : CH_b$

CH_b :Verify $hash(CH_a \| S_b \| S_a)$.

At this point, both mutual authentication completed, and can generate a shared communication key S_b.

(2)Program analysis

In this scheme, CH_a and CH_b need calculate the number of times and communication times are in the following table 2.

Table 2. Node computation and communication times

Nodes	Point multiplication （times）	Times of communication
CH_a	three	send two times，receive one time
CH_b	three	send one time，receive two times

In the certification process, the maximum amount of computing is the elliptic curve point multiplication. This process, two nodes only need three point multiplication. In addition, the program uses a standard challenge response type, three times computation between nodes are the more reasonable process. Contrast to certificate-based protocol, this program has reduced the transmission and validation of the two certificates. Compared with traditional PKI authentication system, the cluster head certification process eliminates the steps to query each other's public key to the management center.

(3)Security analysis

Crack the communication key. The communication key $S_b = d_b T_a = r_1 Q_a = r_1 d_b P$, depends on the random number r_1 selected by CH_a and the private key d_b of CH_b. r_1 and d_b do not appear in the network, only T_a is in the network transmission. Even if the attacker gets T_a, and find Q_b in the public key certificate, but it is difficult to deduce r_1 and d_b by T_a and Q_b. Therefore, the communication key will not be compromised.

Middle attacks.Assume that the attacker C intercepted the request information by CH_a to CH_b, C randomly selected $r_c \in [1, n-1]$ to calculate $T_c = r_c P$, and distribute T_c to CH_b instead of T_a. CH_a Selects r_2 to calculate $S_b' = d_b T_c$, $S_a = r_2 Q_a$,and obtain $h(S_b' \| S_a)$. Then C intercepted the messages CH_b ,to counterfeit CH_b to send $T_c \| h(S_b' \| S_a)$ to CH_a. CH_a receive messages to calculate $S_b = r_1 Q_b = r_1 d_b P$, and $S_b' = d_b T_c = r_c d_b P$, $S_b \neq S_b'$, so verify $h(S_b \| S_a') \neq h(S_b' \| S_a)$.Therefore, the attacker is in no way to impersonate any party communications by the intercepted information.

Repeated attacks.Assume that the attacker repeatedly sends the same message, and looks forward to the different reply to get the user's private key. But through the certification process ,we can find that the reply by CH_a initiating the communication request and verifier CH_b are based on random numbers. This random number is known only by the sender. The random number can guarantee that there is no fixed association between each request and reply. The attacker can not crack the private key by replaying.

In view of a variety of advantages of the elliptic curve cryptography mechanisms [4], the paper designs authentication scheme based on elliptic curve cryptography mechanism as well as the specific implementation process. In wireless sensor networks, each node is artificially pre-placed, fixed in a specific location. Elliptic curve cryptography mechanism needs the public and private key pairs ,they can be assigned to each node in advance. Base station, whether in computing power, the energy reserves in terms of storage space, has a more powerful device than ordinary nodes, so it generally thinks the base station as a key distribution center, to generate the public and private key pairs of elliptic curve cryptography mechanism.

REFERENCES

[1] Yu Li-juan. Analysis and research of wireless sensor network security issues. J. Network Security Technology and Application.2009, 80–82.

[2] ZengYingzhi. Technical Summary of the safety certification of wireless sensor networks. Computer Applications and Software.2009

[3] Xiao Zhiwen. The Study of Elliptic curve digital signature and encryption[D]. Hangzhou:Zhejiang Normal University. 2010

[4] Lin Yubing. The design and implementation of authentication scheme based on elliptic curve in wireless sensor network[D]. Hangzhou:Zhejiang University of Technology,2008.

***Authors**: Xiaorong Cheng, School of Control and Computer Engineering, North China Electric Power University.BaoDing, China. E-mail: Cheng3100@sohu.com; Mingxuan Li, School of Control and Computer Engineering, North China Electric Power University.BaoDing, China. E-mail: 275898849@qq.com*