Secure Communication and the Leak Proof Positioning Technology of Wireless Sensor Based on Region Partition

Xu Min , Li Nige, Hou Zhansheng, Wang Gang, Peng Lin, Han Haiyun, Du Haibo,Zhu Yunyou

State Grid Smart Grid Research Institute

Nanjing, Jiangsu, 210003, xumin1@sgri.sgcc.com.cn

Key words: Private key and timestamp cross certification; High strength encryption algorithm suite; Leak proof private key

Abstract: Power transmission network depends on various sensors to obtain the real-time status of the network, due to the huge number of sensors and random distribution, direct access to the network will bring huge waste of bandwidth resources, and in the process of communication, the key data of the power transmission network and the location information of the alarm sensor are the risk of the external eavesdropping. Therefore, it is urgent to design a set of effective method to solve the problem of transmission efficiency and safety of the power grid, to ensure the normal operation of the network. This paper is based on reducing the burden on the network and improving the security of system access, a secure communication and private key location technology of wireless sensor based on region partition is designed by using the technology of time synchronization verification. The power transmission network in the vast amount of sensor partition, effectively improve the efficiency of power grid data transmission. The risk of leakage of the coordinate mapping table to the grid data information is prevented by the leakage of the private key location technology. Through the private key and the time stamp authentication technology, the security level of the system communication is effectively increased.

1. Introduction

With the rapid development of computer network technology, communication technology, embedded technology and sensor technology, Micro sensor with sensing capability, computing power and communication ability aroused people's great attention.WSN integrated sensor technology, embedded computing technology, modern network and wireless communication technology, distributed information processing technology, it can be through the micro sensor collaboration of the integrated real-time monitoring, sensing and collecting all kinds of environmental or monitoring information, Through the embedded system to information processing, and through the random self organization wireless communication network, the sensing information is transmitted to the user terminal by multi hop relay, In order to realize communication and ubiquitous computing.

The operation safety of power transmission equipment and line is the basis of reliable and stable operation of electric power system. Through the installation of the power transmission line equipment, video equipment and current voltage sensor, Through the mobile wireless network, the operation of the equipment and the line is achieved, and the unified management and unified scheduling is realized. Power transmission monitoring network is an important part of power transmission monitoring system, Its main function is to realize the reliable transmission of terminal data in the network. Network is composed of wireless sensor nodes, which are data acquisition and transmission, Its security has a vital role in the whole monitoring system.

2. Wireless sensor network architecture and secure communication technology based on power shift inspection

The main content of the electric power mobile inspection is to inspect the working state of the power transmission network, relying on all kinds of sensors distributed in the transmission network to obtain real-time state information transmission network. And the distribution of sensors in the

© 2015. The authors - Published by Atlantis Press

power transmission network is on the transmission line, the numerical number and the same region detection will have great similarity, such as temperature, humidity and other environmental values in the same region of the numerical value is very approximate, if the value of each sensor is directly sent back to the server, Will lead to the great waste of sensor communication channels caused by the large number of redundant data acquisition and added to the server's data processing pressure. Therefore, we must design a reasonable center node, partition the sensor partition, each sensor transmits its own data to a central node, which is responsible for each sensor node, analysis of data characteristics of the sensor data from the central node according to the region of the genus, after data redundancy processing, upload the backend server. So it can ensure the data transmission efficiency and accuracy, reduce the impact of a large number of data on the server and the occupancy of the communication channel.

In the actual communication process, it is very important to collect the data of the sensor, power transmission network in the sensor data acquisition is more important, must be encrypted to prevent eavesdropping. But single sensor processing capacity is weak and the number is huge, each sensor is equipped with a separate private key for authentication and data encryption scheme, although the security performance has been improved, however, the energy consumption and the calculation speed of the sensor are increased, according to the characteristics of the sensor domain partition data transmission, in the area of the central node, the private key is equipped with a private key to encrypt the encryption with the time, the security of data in the process of long-distance transmission, as a result of the authentication and the authentication of the signature of the private key with the time stamp, can effectively prevent data in the transmission process of the eavesdropping. Even if the eavesdropper gets the center node of the private key, because of the eavesdropping and server time synchronization is not possible, therefore still cannot pass authentication, thereby preventing eavesdropping illegal hacking of power data. According to the data transmission area sensors reporting center node, using the symmetrical lightweight encryption algorithm, with hardware encryption equipment, using less computational resources and energy consumption, can achieve the realization of sensor data encryption, achieve an effective balance between the efficiency and security. Sensor network architecture as shown in Figure 1, the specific encryption communication steps are as follows:

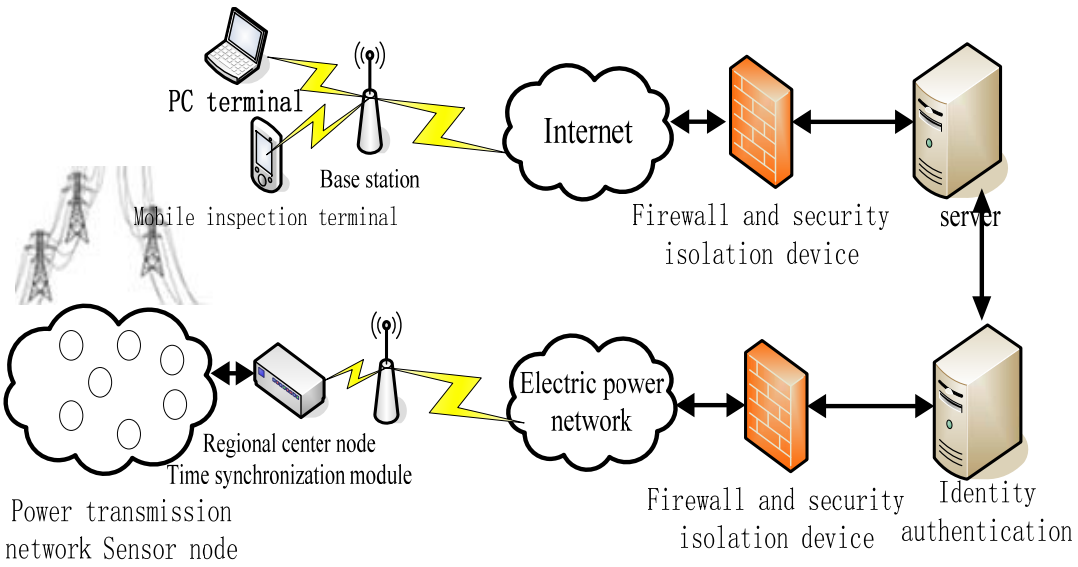

Figure 1 power transmission network sensor network architecture diagram

(1)The sensor sends the information to the center node of the sensor by using a light weight and a symmetric encryption algorithm SM1 algorithm [1]. The sensor sends information contains a unique identifier (uid) to the region node identification code (NodeCode) equipment and sensors to monitor the data information (content), sensor data transmission format as shown in Figure 2.

S	Central node address 8bits	Packet length 4bits	NodeCode 4bits	UID 8bits	Data

Figure 2 sensor data transmission format

(2)The center node receives the information from the sensor and analyzes the information. After identification of the identification code of the nodes in the region, the analysis is conducted, only when a node identifies a code with its own node, the data is imported, otherwise treated as invalid information. After the center node receives the data information of all the sensors in the area, the data feature extraction to obtain feature vectors for each sensor, all kinds of sensor data into meaningful groups, and weighted the redundant information of different sensors, weighted mean value using the least square estimation algorithm [2], finally, the feature vectors of these sensors are fused to obtain the joint feature vector.

(3)After the central node of the sensor data fusion, the use of time synchronization module to send instructions to the server for time synchronization, all the hardware encryption card interface Abstract hash algorithm SM3 pretreatment, and with the system time stamp again hash verification SM3. Finally, the SM2 signature is performed using the private key of the central node [3], Specific process is as follows:

a. The public key of the node identity code and the central node certificate of the center node is obtained by SM3 Z, arithmetic formula: $Z = SM3(ENTL||NodeCode||a||b||xG||yG||xA||yA)$ among them:ENTL bit length of NodeCode is represented by 2 bytes; NodeCode for node identification code; a,b is the system curve parameter;xG、yG as the basis points； xA、yA public key for the user [4][5].

b. Use the Z value and the pending signature message M, through the SM3 hash operations abstract value H. H digital signature for SM2. Arithmetic formula:$H = SM3(Z||M)$.

c. The time stamp T of the central node system is used as the signature information, again using the Z value through the SM3 hash operations abstract value Y obtained. Y digital signature for SM2. Arithmetic formula:$Y = SM3(Z||T)$.

d. Certificate private key with terminal, After the SM3 hash of the information H and SM2 for Y signature algorithm to get the result S,$S = SM2(H||Y)$, after joining the node identification code, the S is passed to the server, specific transmission data format is shown in Figure 3.

(4)The server receives the information from the center node, the information packet is decomposed, read the encryption kit signs, Select the specified encryption algorithm, called the hardware encryption card interface SM3 digest algorithm will be the local certificate after the hash, and then use the SM2 algorithm to verify the information. Specific process is as follows：

a. The public key of the node identity code and the central node certificate of the center node is obtained by SM3 Z, Arithmetic formula:$Z = SM3(ENTL||NodeCode||a||b||xG||yG||xA||yA)$.

b. Using Z value and the M to be signed message, the H is obtained by SM3 hash operations. H digital signature for SM2. Arithmetic formula:$H = SM3(Z||M)$.

c. Gets the server system time stamp T as the pending signature, again using the Z value through the SM3 hash operations abstract value Y. Y digital signature for SM2. Arithmetic formula:$Y = SM3(Z||T)$.

d. Using the public key of the gateway server, the SM3 and H are combined with the Y after the pre - processing, And the signed value S signed by the central node SM2 is the result of the Q test, $Q = SM2(H||Y||S)$, and judge whether the value of Q is true, If true, the central node's certificate is valid. If it is not true, the certificate of the central node is illegal, and the connection between the central node and the central node is interrupted.

e. After verification, the central node sends the information of the sensor to the back of the authentication server.

server address 8bits	Packet length 4bits	NodeCode 2bits	SignatureValue(S)32bits	Encryption Kit 2bits	Private key hash 256bits	Sensor position 8bits	Data

Figure 3 center node data transmission format

(5)After receiving the authentication information of the central node, the server is in the work network, Using encryption suite sign bit specifies the symmetric encryption algorithm SM1 coming from the central node to decrypt encrypted information operation. Finally, it obtains the field sensor by fusion after processing the monitoring data center node.

3. Wireless sensor based on private key positioning technology to prevent leakage localization technology

After the mobile terminal is found through the mobile terminal, the most important is to find out the route node which is the fault of the transmission line, In order to use the fastest speed to go to the site for maintenance work, So the wireless sensor positioning technology has become an important research direction. The simplest method is to install the sensor's position information on the sensor GPS device, however, the sensor of power transmission network has the characteristics of huge quantity and the change of position after installation is not obvious, For each sensor installation GPS module will obviously huge cost and subsequent maintenance work will be very cumbersome, therefore, it is necessary to develop a set of effective methods can not only save the cost and accurately informed of the sensor position and stop hackers from external get position information of the sensor, power grid to prevent critical data breach.

Aiming at the characteristics of large quantity and location of power grid sensor, can use the private key to locate the wireless sensor to prevent leakage localization technology, meet the requirements of the power grid for sensor positioning and leak proof. The central node server, which has a small number and distribution, is in the process of installing the server, using the GPS module to measure the position, and record, associated with a unique private key certificate hash code for each central node, generating center node distribution, For a large and distributed random wireless sensor, the position of the sensor relative to the center node is measured by using the APIT localization algorithm [6], as shown in figure 4, after the weighted calculation of the center node distribution map, we can know the exact location information of the wireless sensor.

The APIT algorithm is a distance independent and a region dependent localization strategy. In fact, is simple, low cost, low power consumption, low power consumption, high positioning accuracy, so it is widely used. As shown in Figure 4, it is the basic algorithm to choose from the anchor nodes around the nodes around the three arbitrary, combined into a triangle, to determine whether the point is located in the triangle. If in a triangle, the marker, followed by treatment anchor node localization around the various combinations and detection, finally find out that meet all requirements of the triangular overlap region, for the centroid position to replace the unknown nodes in the network specific location coordinates.

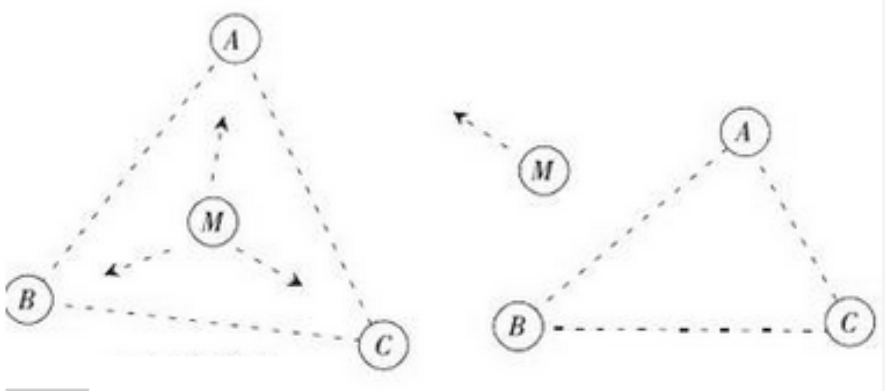

Figure 4 APIT schematic diagram

Specific positioning steps are as follows:

(1)The device installer installs the wireless sensor to the corresponding node location, and sets the center node area corresponding to it.

(2)Installation personnel to install a central node server, using GPS module to get the server coordinates information g, uploaded to the server, central node automatically using the corresponding private key s hash to get the value of H, Arithmetic formula: H = SM3(S), and the abstract value H is sent to the server.

(3)After the installation of the installation of all the central node, the server to gather all of the central node of the {Hn} and the {Gn} of the coordinates of the installation of the installation of the data array, associated with the coordinate information of the private key, the coordinate mapping table is generated automatically, as shown in Figure 5.

$$\begin{Bmatrix} SM3(S_1) & \cdots & SM3(S_i) \\ \vdots & \ddots & \vdots \\ SM3(S_j) & \cdots & SM3(S_n) \end{Bmatrix} \times \begin{Bmatrix} G_1 & \cdots & G_i \\ \vdots & \ddots & \vdots \\ G_j & \cdots & G_n \end{Bmatrix}$$

Private key hash value	Coordinate position
H4D1DSCD2QWDEW…	(118.543,32.043)
XSACSCSD324R4F4…	(118.214,32.333)
E32ETVFD34RF43G…	(118.346,32.543)
D34G54G45G54G34…	(118.814,32.313)
SD34GDDS45G5CSS…	(118.812,32.343)
…….	…….

Figure 5 table generation process

(4)Data fusion analysis is performed after the central node receives the data information from the sensor, A sensor value for monitoring data is beyond the warning, using APIT positioning algorithm, The calculated alarm sensor relative to the sensor node relative location information center.

(5)The center node is in the process of communicating with the server as shown in Figure 3, In addition to sending the node identification code, signature information, encryption suite identification code outside, the private key also added a 256 bit hash value and 8 sensor relative position information, after the server receives the hash value, automatic matching coordinate mapping table, in order to obtain the position information of the central node, according to the relative position of sensor information weighted calculation, accurate location information and to obtain alarm sensor.

(6)According to the system settings, the private key of the central node is updated regularly, so even if the internal coordinate mapping table information leakage, once the private key update is completed, the center node and sensor location information of the alarm can still be obtained according to the old mapping table, to effectively guarantee the safety and reliability of power transmission of information.

4. Summary

This paper presents a wireless sensor communication security and anti leak positioning technology by private key regional division of state secret Bureau authentication encryption algorithm and time synchronization technology based on parity. Partition of large amount of sensor in power transmission network, fusion of sensor data with central node, eliminate redundant data, effectively improve the efficiency of power grid data transmission, reduce the redundancy of the detection data to the extent of the bandwidth of the. Through the application of the encryption algorithm, the time synchronization verification technology is added to the identity authentication signature algorithm, effectively increase the security level of the system communications, to prevent external hackers

access to the network access to important information network. Through the bundle of the private key and the position information, eliminate the traditional way to coordinate the device number and coordinate to bring the following coordinate mapping table revealed hidden trouble, The key update preventing leakage coordinate mapping table to bring the loss of the grid data information. Through the use of APIT algorithm, the relative displacement of the sensor and the center node of the region are calculated, according to the center node coordinates to calculate the specific location of alarm sensor, effectively reducing the cost of wireless sensor positioning, greatly improves the anti eavesdropping ability of power network data.

Reference

[1] State Password Administration．Certificate authentication system password and related security technology specification．2005．

[2] Wang jiangang, Wang fubao, Duan weijun. Application of weighted least square estimation in Wireless Sensor Networks [J]. Computer application research. 2006(09)

[3] State Encryption Administration. SM2 elliptic curve public key cryptography algorithm recommend curve parameters [EB / OL]. www.oscca.gov.cn/UpFile/2010122214836668.pdf,2010.

[4] Liang Wu seven; based on elliptic curve public key cryptography and its application [J]; Anhui Radio & TV University; 2011 01

[5] Darrel Hankerson, Alfred Menezes, Scott Vanstone. Guide to Elliptic Curve Cryptography. New York :Springer-Verlag, 2004.

[6] Wang Q, Ren K, Yu S C, et al. Dependable and secure sensor data storage with dynamic integrity assurance[J]. ACM Transactions on Sensor Networks (TOSN), 2011, 8(1): 1-24.