Research on Reconfigurable Key Management in Electric Power Communication Network

Huan Li[1, a] , Shengyang Lu[2, b], Wei Li[3, c] Hongbi Geng[4, d]

[1,2,4]No.39, Siping Street, Heping District, Shenyang, Liaoning,China. Electric Power Research Institute

[3]No.18, Ningbo Street, Heping District, ,Shenyang, Liaoning,China. State Grid Electric Power Co., Ltd. in Liaoning Province

[a,b]13555868244@126.com, [cd]840236868@qq.com

Keywords: Ectric power communication network, Information security, Reconfiguration, Key management

Abstract. With the development of electronic communications technology. Intelligent devices are widely used in electric power communication systems, smart substation gained rapid development. The intelligent electronic devices all use equivalent way to connect in smart substation, this way improved the interaction and sharing of information, but it also brings security risks. In order to protect the network information security, It proposed a reconfigurable key management combining with the characteristics of electric power communication network.

Introduction

With the continuous development of science and technology, the grid business and kind of access terminal are increased, smart network has become an inevitable trend of network development.Smart grid take the existing of high-speed, two-way network as basis,Then used application of the sensor technology, measurement technology[1], equipment technology, control method, and decision support systems to achieve reliable, economical, safe, efficient, environmentally friendly and safe target in power grid.As the smart grid substation is the important node of power grid, responsible for important task of selectricity transmission and distribution, therefore, whether substation can make information safe and reliable transport, is essential for stability and reliability of the power system[2]. In order to ensure the safety and effectiveness of inter-substation communication, it needs to be encrypted and authentication, and key management is the basis for all security encryption. The adaptive management of key reconstruction would ensure the safe and efficient network, to extend the lifetime of the network, reduce interaction latency, optimize network performance when the substation node fails.

Key Management

(1) Key Management Overview

Modern cryptography believes that the security of the cryptographic is not confidential of algorithm itself, and that security is the authenticity and validity of the key. Key management techniques focus on solving a variety of security technologies based on cryptography used in the key, involves key generation, management, distribution, storage, updating, cancellation, destruction throughout the life cycle. To ensure security, the key is to design a secure and efficient key management scheme, in order to lay a solid foundation for the implementation of other security mechanisms.

(2) Key Management Categories

According to the forms of CA[3-4] existing in the network topology, management scheme can be divided into three categories: centralized key management, distributed key management, hierarchical grouping key management.

In the centralized key management, it selects a stable and relatively high credit value node is responsible for key generation, distribution and updating in the entire network.Usually this selected node is called the root[5]. The advantage of using this kind key management is beneficial to the management of network traffic, it can be more easily applied to identity authentication, key distribution and other measures. But such centralized key management dependences on the root too large to lead to a single node failure problem.And root node may also be bottleneck of the network, as the large cost of a safety network, which would affect system performance.

In distributed key management[6], in the network initialization phase, the offline CA center apply threshold scheme (k, n)[7] to distribute CA to a group of dedicated server nodes.Each server node can be generated certificate section using a secret share. While k such certificate compose to get a complete valid certificate, those k server nodes can act as CA. It can avoid safety problems of a single CA node, While this scheme during the certificate application and renewal node, a node needs to send an application to at least k nodes, and also have to receive at least k service nodes certificate in order to complete the application or renewal process, which would the computational overhead of the network.

Hierarchical grouping key management[8] is divided all nodes into several groups, each containing different levels. There is a control node in each group, and these nodes will be able to compose key level *I* in management scheme, while the remaining nodes of the key management group compose level *II*. These two levels can independently choose its network management standard and programs, such as the use of centralized or distributed management, while the manner in which inevitably will inherit advantages or shortcomings of these approaches at each level. For example, in the level *II*, it usually uses centralized control type if the number of members within the group is small. While the group size is still relatively large, the notes can divide into new groups to generate a new level.

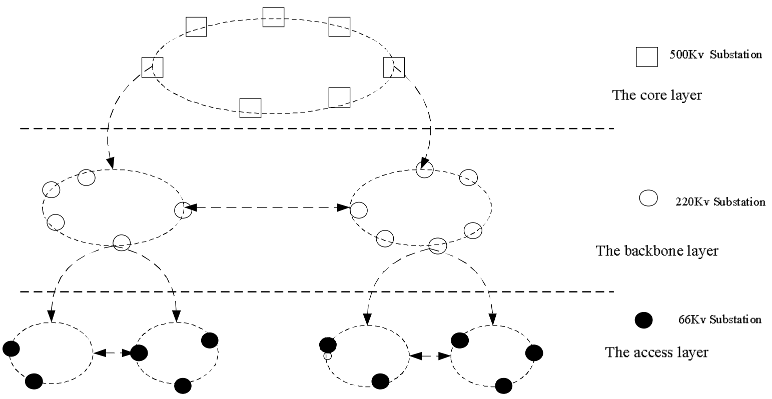
Authenticity[9]. Certification requirements for external attackers even be able to monitor all network traffic within the network and tries to fake members, they can not calculate the system key. Certification guarantees only the group members can calculate the public and private key, public key for authentication, the private key for encryption.

Forward secrecy. When a new node joins the network or the current key compromise, forward secrecy can ensure the security of the key used in the past.

High communication efficiency[10]. Since the distance between the power communication network notes is farther, it will make higher communication delay and bit error rate, and therefore it needs to establish a high communication efficiency and fewer communication rounds of the program.

At the stage, the key management research focuses on how to ensure the dynamic changes in the network environment to achieve safe and effective key generation, update and distribute, so that nodes join or leave the network and when attacked ,it can not only ensure the independence of each key update, also can reduce the cost of network communications and computing, and saving network resources .

Reconfigurable key management Network Initialization, it puts forward asecurity architecture with the feature of electric power communication network in Reconfigurable key management, security architecture divided into the core layer, the backbone layer and access layer. In the initialization phase, the core layer, the backbone layer, the access layer are all using centralized key management.



Network

Figure 2.1 Logical hierarchy of Power Communication

Generate keys-Control Center is responsible for generating total system private and public key, as well as the public and private key for each substation node. The control center need save the key for all nodes in the network, while the rest of network nodes only need save itself private key and all nodes public key.

Produce certificate-The network nodes need a certificate to prove the validity of the theirselves, the format of the certificate cert = *<ID_i, PK_i, Version, Tvalid, Server-flag, Issuer, (r, s), w>*. Control center issued a certificate in accordance with the legality of the node.

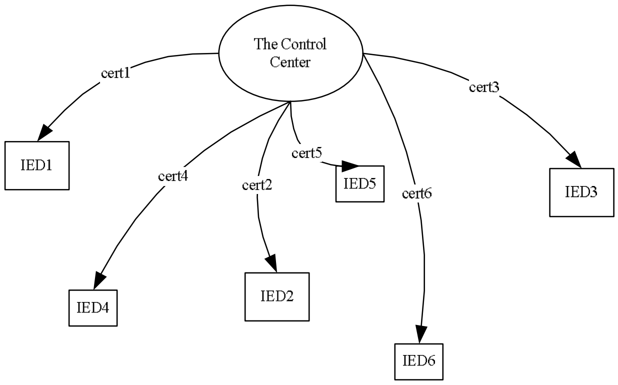


Figure 2.2 Control Center Distribution Certificate

Certificate update-In order to ensure network security, It need update certificate periodically. Control center generates the new certificates for other nodes, the key is different from to the front to meet the confidentiality, while the certificate number is updated, once plus one, the original certificate expires.

(3) Key Management Reconstruction

When the control center fails, resulting in authentication and encryption can not be achieved in the network, then the network would start key management remodeling. According to the hierarchical organization of the electricity network, the core layer uses distributed key management scheme, the backbone layer nodes,as leaf nodes of the core layer, use the core layer nodes within the communication as the control center, the access layer nodes use backbone nodes as a control center.

When the core layer substations have not received new certificate send by the control center in the time *T*, each core node would calculat credit for each core node according to a list of allegations.

Table 2.1 Allegations Node Lists

Node	Accuse/time	Be accused/time	Time
ID_1	X_1	Y_1	$\{t_1 , t_2 ... t_{x1}\}$
ID_2	X_2	Y_2	$\{t_1 , t_2 ... t_{x2}\}$
....	...	...	...

In calculating credit, adding impact factor, nodes accuse and be accused will affecttheir own credit, as shown in table 2.1, in order to encourage the faithful nodes accuse of malicious nodes, factor $k_1 < k_2$.

$$W_i(t)=W_i(t-1)-k_1x_i-k_2y_i \tag{1}$$

Based on credit value, select n core layer nodes as server nodes. Server nodes could provide new certificate for other common network node, new certificate can be used for encryption and authentication between nodes.

In order to ensure inter-network security, the core layer nodes will communicate monitoring malicious or anomalous behavior of its neighbors during network operation.Then they form a new list of charges in 5T time and calculatecredit value to elect new server nodes.

In backbone and access layer node, the core node provided certificate update service periodically, each certificate update need to get certificate fragmentation issued by the core layer nodes, at least k fragmentations can make up the new certificate, and certificate plus one to a version number, in order to ensure safe communication between nodes, only the same version number of the certificate can use for authentication and encryption between nodes.

If the access layer nodes want to communicate with each other with different certificate version number, in order to save communication resources, reduce communication latency, they can apply their common access layer node to provide public and private key for this communication, complete authentication and encryption.

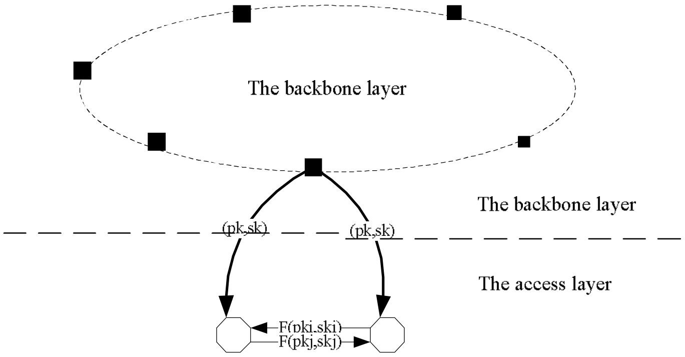


Figure 2.3 Encryption and Authentication in Access Layer

Feasibility Analysis

According to the characteristics of electric power communication network, it propose reconstruction of key management to meet the dynamic changes of the network to ensure the safe operation of the network. In the network, considering the network operation status, it is divided into the core and access layer reconstruction. While, in different key management scheme, according to different programs with different mechanisms, adding trust list to ensure that network adaptive process variation. It uses mutual supervision between nodes to detect and eliminate the malicious nodes, In the access layer, it uses slave node authentication mechanisms to reduce delays, save network bandwidth,ensure the network information security, optimize network performance.

References

[1] Qiang Gao, Xianwei Liu, Lijun Qiu, "The emergency communication network and its anti-destroying ability analysis of the electric power system," Electric Power Grid Technology. 2009.

[2] Wenqing Chen, Qingfeng Ma, Jianli Zhao, "The reliability evaluation method research on the electric power optical fiber transmission network," Electric Power System Communications. 2011.

[3] Lynch K M,Schwartz I B,Yang Pet , "Decentralized environmental modeling by mobile sensor net-works," IEEE Trans. Robotics , 2008.

[4] Tsz Hon Yuen,Willy Susilo,Yi Mu, "How to construct identity-based signatures without the key escrow problem". International Journal of Information Security . 2010 (4)

[5] LIU Yanmin, SHI Jianjun, "Mutualauthentication and key exchange scheme based on SRP," Computer Engineering . 2004 , 30 (16): 42 - 44.

[7] Zheng Huanhuan, "MANET No certificate key management research," Xi'an University of Electronic Science and Technology .2012.

[8] Garcia E,Colorado C A.System and method for communicating with a key management system. US, US8667267 B1 . 2012

[9] G.Yang, J.T.Wang, H.B.Cheng, "Wireless sensor network key distribution method based on identity encryption," The Chinese Journal . 2014.

[10] Z.G.Qin, Z.J.Li, J.H.Wang, "Research on wireless sensor network key distribution protocol," Computer science . 2014.