LOU YONGMEI
WANG YING
and
LI GEN

A new authentication scheme and enhance authentication protocol for large scale metering in smart grids

Advanced Metering Infrastructure (AMI) plays an important role in the development of the smart grid. AMI is a computer network, which has to face the cyber security issues inevitably. Safety certification is one of the many cyber security issues. AMI have a lot of accessible devices, therefore it needs a simple and secure access mechanism. IEEE 802.1x is widely applied in solving the problem of wireless LAN users access authentication. In this paper, we propose a modified version of IEEE 802.1x protocol to meet the special requirements of AMI. In addition, we applied the modified IEEE 802.1x protocol also in our newly designed AMI architecture based on IPv6, and discuss the details of the authentication process. Finally, we build the experimental environment. We realize the design of AMI architecture in this experiment, and use the authentication mechanism proposed in this paper in it. Experiments show that the proposed authentication mechanism can meet the special needs of AMI, and our newly designed AMI architecture based on IPv6 has a direct commercial value.

Keywords: *Smart grid, Advanced Metering Infrastructure, sensing architecture, authentication protocol, IEEE 802.1x, SCEP*

1. Introduction

Smart grid is of great significance for the energy efficiency improvement, distributed energy grid integration, dynamically adjustment of the power load, and user interaction enhancement, thus it is a key part of the development of the next-generation energy Internet. Advanced Metering Infrastructure (AMI) is a bidirectional communication network, which provides communication and data collection architecture for the smart grid infrastructure [1, 2]. In addition, AMI is a computer network so that cyberspace security problems still exist. AMI also faces cyber security challenges, such as security authentication, secret key management, secure data transmission and storage, intrusion detection, etc [3]. Liu N et al [4] proposed a new secret key management mechanism, which can apply to unicast, broadcast and multicast, based on analyzing the characteristics of AMI and the difficulty of establishing secret key management mechanism. Based on the data collection from the smart meter, Azghandi S et al [5] presented an empiricism security model for encryption and secure data transmission process. Faisal M A et al [6] analyzed seven kinds of AMI intrusion detection algorithms based on the data flow which provides useful data for AMI intrusion detection. Nicanfar H et al [7] proposed the efficient SG Mutual Authentication (SGMA) and SG Key Management (SGKM) protocols, for the existing security authentication and certificate management problems in IPv6 protocol and meshed AMI architecture [8]. SGMA uses identity-based authentication, which reduces the steps of authentication in the Secure Remote Password (SRP) protocol from 5 to 3. SGKM protocol uses EIBC (enhanced ID-based cryptography) mechanism to reduce the overhead of updating the secret key. These two mechanisms have good defensive performance for common attacks such as brute-force attack, replay, MITM, DoS. Fouda M M et al [9] designed a smart grid communication framework, and based on this framework, they proposed a lightweight message authentication scheme that uses Diffie-Hellman key exchange protocol and a hash-based message authentication code to achieve mutual authentication deployed in electrical equipment and communication systems in different regions.

IEEE 802.1x is an access control protocol based on port, and it is widely applied in solving the problem of wireless LAN users access authentication [10]. Extensible Authentication Protocol (EAP) is used for device authentication, and EAP protocol is used for data encapsulation in the process of authentication, to ensure the transmission security in the network. IEEE 802.1x protocol achieves access authentication for the users by the port switch control. Before the user finishes authentication, he can only access to the server using an open non-controlled port, and this user is not allowed to access other resources before the authentication process is finished. After the user has successfully authenticated, the server establishes a logical channel through a controlled port on the server, then the user can access network resources through this logical channel.

AMI is a wireless sensor network, also can use the IEEE

Ms. Lou Yongmei, School of Computer Science and Technology, Tianjin University, Tianjin, Mr. Wang Ying, Troops, and Ms. Li Gen, School of Electronics and Information Engineering, Tianjin University, Tianjin, China.

802.1x protocol for authentication access devices [11]. In IEEE 802.1x protocol, EAP plays an important role in the authentication. However, the several existing EAP authentications are not suitable to apply to the AMI. EAP-MD5 (Message-Digest5), a kind of one-way authentication, is unable to provide the two-way authentication between a client and the server [12]. EAP-TLS (TransPort Level Security) is based on the bidirectional certificate authentication, but there are cumbersome steps such as shake hands four times in the process of authentication. In addition, EAP-TLS needs install and maintain certificates on both ends of the client and the server, which significantly increases the workload to the administrator. EAP-TTLS (Tunneled Transport Layer Security) is a two-way authentication protocol, which completes authentication by establishing a TLS tunnel. In this way, a client does not need a certificate. EAP-TTLS reduces the workload by omitting certificates which are necessary in EAP-TLS, but decrease the security at the same time. There are a lot of studies on IEEE 802.1x authentication algorithms. Park K Y et al in [13] analyzed the mobile routing security leak which exists in IEEE 802.1x protocol for wireless local area network, and proposed the trusted platform module to solve this problem. Chi K H et al in [14] proposed fast handoff security architecture on the wireless mesh network.

SCEP is established by Cisco Company, which is a certificate-based authentication protocol. The user's identity, the entity's public key and digital certificates are bound to cryptographically communicate by using PKCS #7 protocol. In addition, the certificate enrollment in SCEP is an online process, which provides a certificate of automatic registration function. SCEP is widely used in network authentication process.

IEEE 802.1x can realize port resource effective isolation using the wireless network control, which provides a solution for AMI network resources isolation [15]. In this paper, we improve IEEE 802.1x protocol, in the way that use SCEP instead of the existing EAPs to meet the special requirements of AMI considering not only the fixed long-term authentication requirements of smart grid terminals (such as smart meters), but also the temporary access of mobile intelligent network terminals (such as intelligent electric cars). The modified IEEE 802.1x protocol has a simplified authentication procedure, which can strengthen the authentication process automation and reduce administrator workload. In addition, in this paper, we apply the modified IEEE 802.1x protocol on our newly designed IPv6-based AMI architecture which can be directly commercialized.

This article is organized according to the following structure: The overview of SECP is introduced in Section I. In Section II, we analyze the special security needs in AMI, and then propose the modified IEEE 802.1x protocol, which is based on the analysis on the demand for the safety authentication and the lack of the existing authentication protocols. In Section III, we design a new AMI infrastructure based on IPv6 and discuss the detail authentication process based on the modified IEEE802.1x-based authentication. Section IV summarizes the full paper.

2. The new authentication mechanism

2.1 The Security Requirements of AMI

Same with other communication networks, AMI faces security threats, such as the middle attack, communication information interception, stored data theft and other issues. However, in addition to the general security requirements, AMI also has some specific security requirements.

2.1.1 Physical security

Physical security of smart meters should get attention. Smart meters are in a special physical environment, so they are easily affected by harsh environment [16]. The climate difference between southern China and northern China is very large, which makes smart meters have very different environments. In many cities which are located in the southern China with poor conditions, meters are usually exposed outdoors so that they are often subjected to high temperatures and rain invasion. What is more, the environment in the southern China is very humid. However, in the north, the smart meters placed outdoors are vulnerable to damage by lightning, rain and snow. In addition, smart meters are moving in the direction of wireless technology, so that space electromagnetic signal interference, and the signal reflection and diffraction by surrounding buildings need to be considered [17].

2.1.2 Certified security

AMI needs to access smart grid devices for authentication, including smart meters, smart routers, etc. Any device accessing AMI must be certified, to prevent middleman attack and forged identity access [18]. Fig.1 is based on the certificate of AMI certification process diagram. The smart grid device sends the authentication request to RA. After confirming the safety of the equipment, RA examines and approves the request and then sends a certification request to CA. After the CA certificates for the smart grid device, the device can access to the communication network of AMI. In

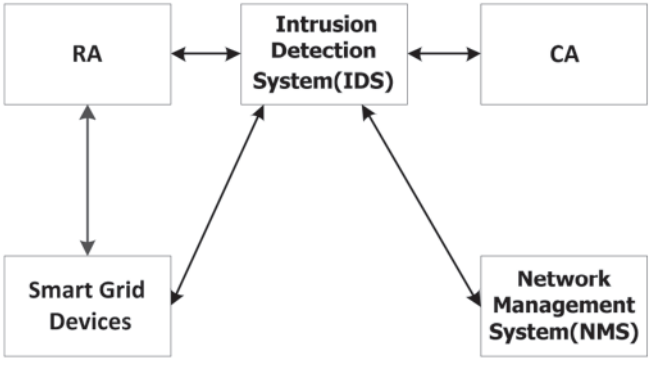

Fig.1 Diagram of based on the certificate of AMI certification process

the diagram, the intrusion detection system is used to detect the attacks in the data packets which flow into the communication network of AMI, such as the DOS attack.

Since the bandwidth of AMI communication network is relatively low, the traditional complex certificate authentication process is not suitable for AMI [19-20]. New authentication method needs to be presented. In addition, with the development of smart grids with mobile terminals, AMI authentication security should also consider charge for mobile terminal users when they require outdoor power support temporarily. Such as in electric vehicle temporary charging process, electric cars should be connected to the grid with the complete authentication process, and be built.

2.2 The Proposing of the Authentication Mechanism

Through the analysis of the special security requirements of AMI, this paper proposes a new authentication protocol, which uses SCEP to replace the existing EAP in IEEE 802.1x protocol. The flow chart of this mechanism is shown in Fig.2. Not only does the authentication protocol apply to fixed long-term access to the smart grid terminals, but also is suitable for temporary short-term access smart grid mobile terminals. The authentication protocol keeps the AMI isolated from unauthorized device, which increases the security of the network resources. In addition, SCEP reduces the workload of the administrator by processing certificate request online.

IEEE 802.1x protocol uses Extensible Authentication Protocol (EAP) standards authentication, but does not provide a specific authentication protocol. Therefore, IEEE 802.1x protocol can have many extendable authentication ways. For AMI in smart grid, this paper proposes an extending version of IEEE 802.1x authentication protocol based on the SCEP protocol. In this way, before finishing authentication procedures, intelligent electric network devices (such as smart meters, smart appliances, charging cars, and etc.) can be isolated from the AMI network resources. The advantage of this authentication protocol is to enhance the AMI network data protection function. In particular, for those smart meters using mesh technology to access to network in AMI, only successfully finishing the authentication procedures, can they access to the mesh network and communicate with other smart meters in the mesh network, or connect to the host by other smart meters routing [21]. In this way, the possibility of master station invaded can be reduced. The authentication process of the modified IEEE 802.1x protocol by using SCEP is briefly described as shown in Fig.3. In Section IV, the detailed smart grid security authentication and the analysis of authentication process in AMI based on this authentication protocol are given.

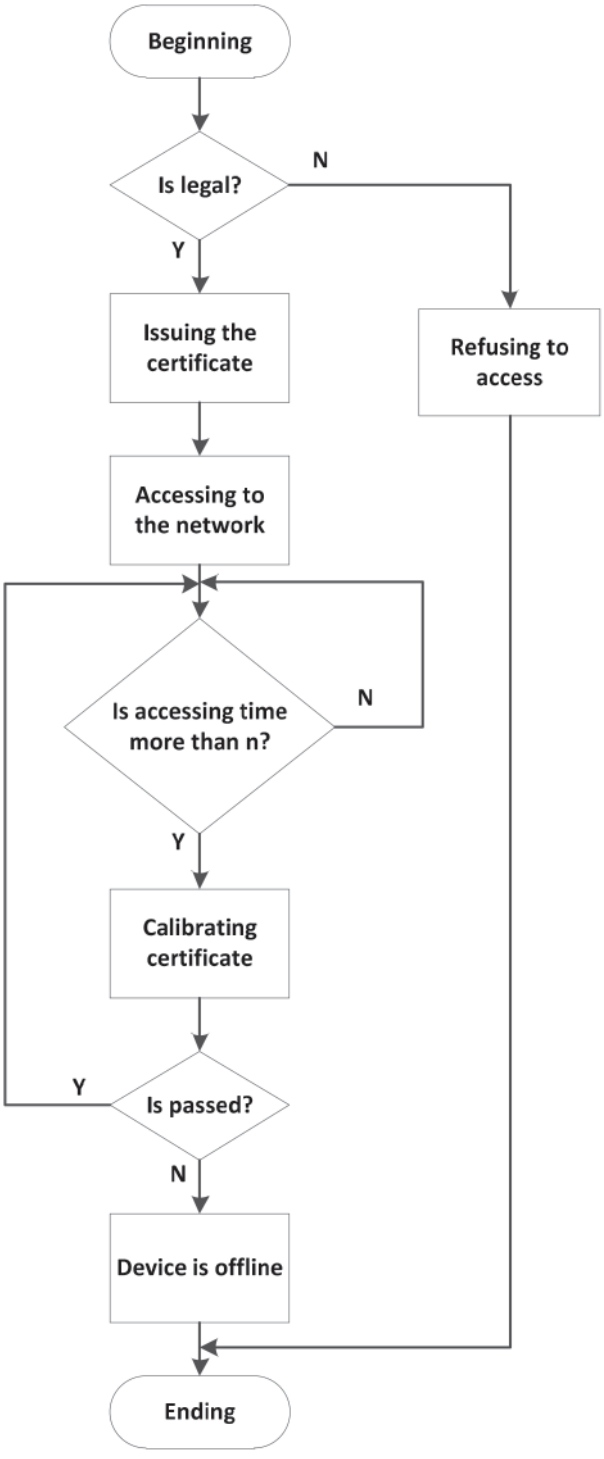

Fig.2 Flow chart of the new authentication mechanism

3. The realization of the new protocol based on IPv6 AMI

3.1 Overview of AMI Architecture Design

In this paper, the design of AMI architecture based on IPv6 is shown in Fig.4. The AMI architecture uses the 6LoWPAN protocol [22] to assign each smart meter an IPv6 address. The RF mesh technology is applied in smart meter networks [23]. The new authentication protocol proposed in section II is adopted by this scheme to be the way of safety authentication. In Fig.4, convergence router is the AP router in the IEEE802.1 x protocol, which is responsible for the use of controlled port forwarding all authentications. If smart grid

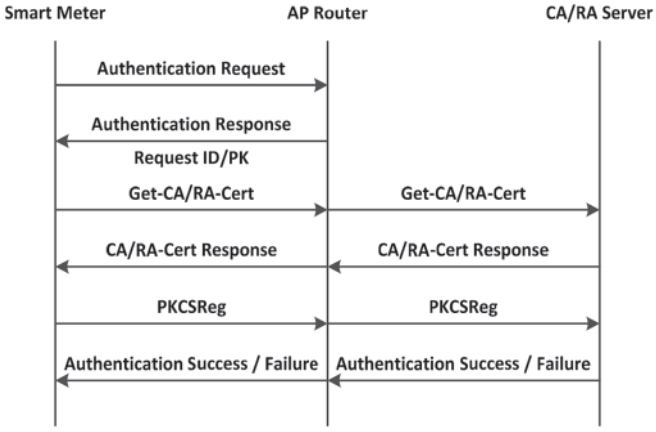

Fig.3 Authentication process diagram of the new mechanism

terminal is successfully certified, the convergence router opens controlled port. Before access to the smart grid, every smart grid terminal needs to send an authentication request to convergence router. Before the authentication through, it cannot use mesh technology to connect with other smart grid network terminals, also not be able to access other resources in the grid. In the authentication process, the smart grid terminal seeds request authentication to convergence routing. After convergence routing allows the authentication request, and sends the SCEP certificate request packet, the router will forward it to RA. After RA finishes reviewing, SCEP message is forwarded to CA through the firewall filtering. After authentication and calculation by CA, CA sends the certificate to the smart grid terminal in accordance with the original way. After receiving the certificate issued by the CA, the smart grid terminal registrants the certificate to the CA's LDAP server, and then the authentication process is completed. After this step, the convergence router opens the controlled port for the smart grid terminal. Then the logical communication channel is established and the terminal is allowed to connect with other terminals by mesh technology, and with the NMS.

For smart meters multiple-hop mesh network, each meter can be used as a transfer of message relay. In this scheme, in order to reduce the burden of computation and storage, the

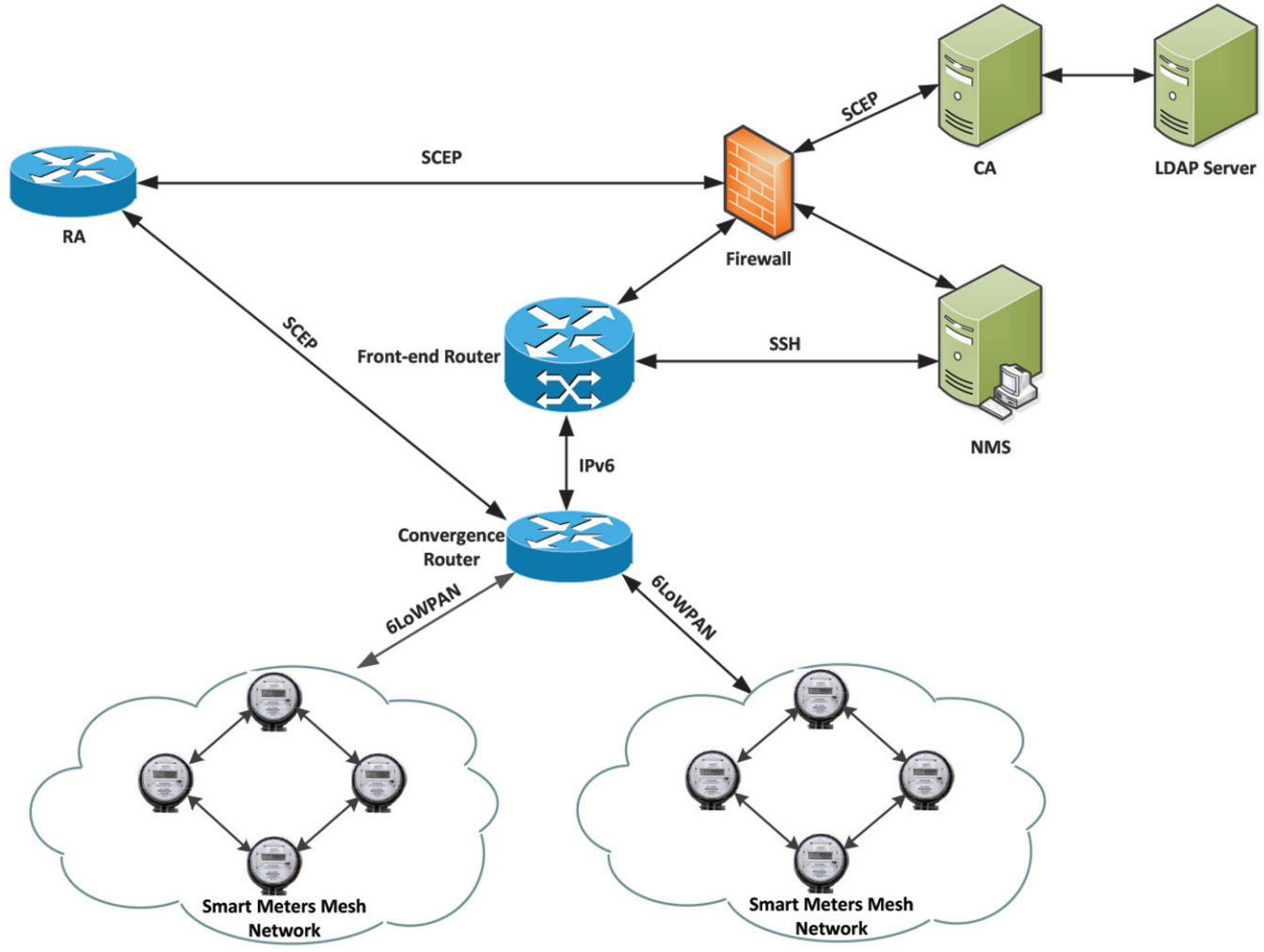

Fig.4 AMI architecture design diagram

routing table from each smart meter to the convergence router is stored in the convergence router. According to the low power loose network Routing Protocol (RPL), convergence router calculates the optimal routing table to each meter, and then inform each smart meter in the routing table which the next-hop meter is. If a meter left the mesh network, convergence router needs to recalculate the routing table. Using mesh networking technology enhances the robustness of the smart meters network.

NMS receives packets through the firewall filtering, and sends a heartbeat packet to each of the smart grid terminal regularly, so as to confirm that the smart grid terminal remains in the activated state. If NMS could not timely receive the heart reply packet from the terminal, it thinks the terminal is not in the network. NMS can also remotely control the login of the front-end routers via SSH, and does not have to be near the front end router, and can carry on the management.

3.2 Design of enhanced authentication for large scale metering

This paper chooses IEEE 802.1x-based SCEP as security authentication protocol in AMI which is designed in this paper. Smart grid terminal is the entity of SCEP protocol, including smart meters, smart appliances. High processing capacity router plays a role as RA, to deal with SCEP authentication request submitted by the smart grid terminal. CA authentication server is behind the firewall. The firewall filters the source IP address, destination IP address, the packet agreement, etc., to ensure that the CA server receiving packets are from the smart grid terminals with secured IP addresses to reduce the risk of the CA server invaded.

The new authentication protocol is extended mainly used the certificate authorizing and the certificate registration in SCEP, which provides a new concrete authentication in the IEEE 802.1x protocol. The authentication mode is more suitable for smart grid system of AMI. According to the design procedure of safety authentication, convergence router provides the functionality of AP in IEEE 802.1x protocol. Instead of a smart grid terminal, convergence router sends access request, certificate authorizing request and registration of SCEP certificate request. However, smart grid terminal certificate query and certificate revocation has not extended to the IEEE 802.1x protocol, consistent with the original SCEP protocol. This scheme is implemented as follows: the convergence router will send SCEP certificate query and revoke request of intelligent terminal to the front of the router, and then front router forward sends the requesting packets to the CA and LDAP servers, so as to realize these two functions.

The different parts from the original SCEP protocol should be main narratives, includes certificate authorizing and the certificate of registration. Fig.5 shows the flow diagram of certificate issuance in the modified IEEE 802.1x by using SCEP, which is taking the smart meters as an example. The detailed description is:

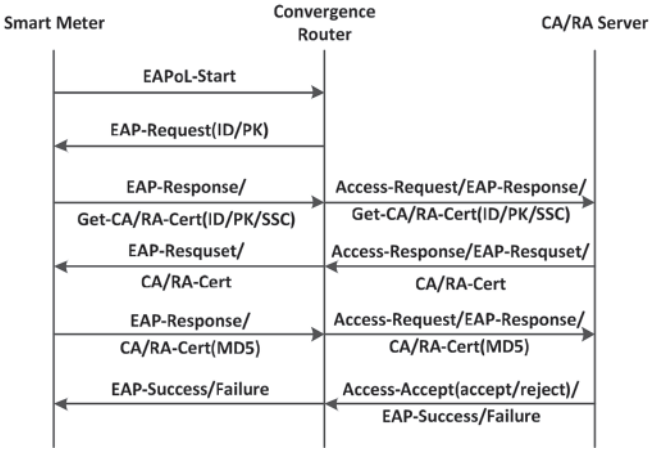

Fig.5 Sequence diagram of certificate issuance in the modified IEEE 802.1x by using the SCEP, which is taking smart meters as an example

(1) Smart meter sends access request to convergence router, then convergence router returns a response that asks the smart meters to upload its ID and its public key.

(2) Smart meters issues a certificate authorizing request, and attached its ID, PK and self-signed certificates (SSC) which is formed by its ID and PK in the request.

(3) CA/RA server receives the convergence router forwarding certificate request, and verifies the SSC by using PK for authentication. If authentication is successful, the certificate can be issued. At the same time, the CA encrypts the ID number and certificate request operation number in SSC, by using PK, and then sends the cipher text to the smart meter.

(4) After receiving and decrypting the cipher text forwarded by convergence router from CA/RA, the smart meter sends a MD5 fingerprint generated from its local private key to the CA/RA.

(5) After receiving the MD5 fingerprint, CA/RA verifies it. If the validation is success, the certificate authorizing is success. If verification is not success, the certificate authorizing is failure.

Certificate registration procedure is relatively simple, as shown in Fig.6. After a smart meter sending a certificate registration request, convergence router transmits this request to CA/RA, and after CA/RA approvals the request, certificate registration is successful.

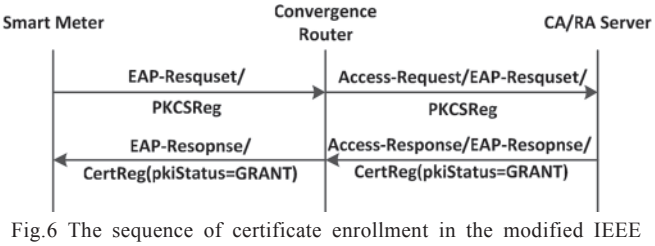

Fig.6 The sequence of certificate enrollment in the modified IEEE 802.1x by using the SCEP, which is taking smart meters as an example

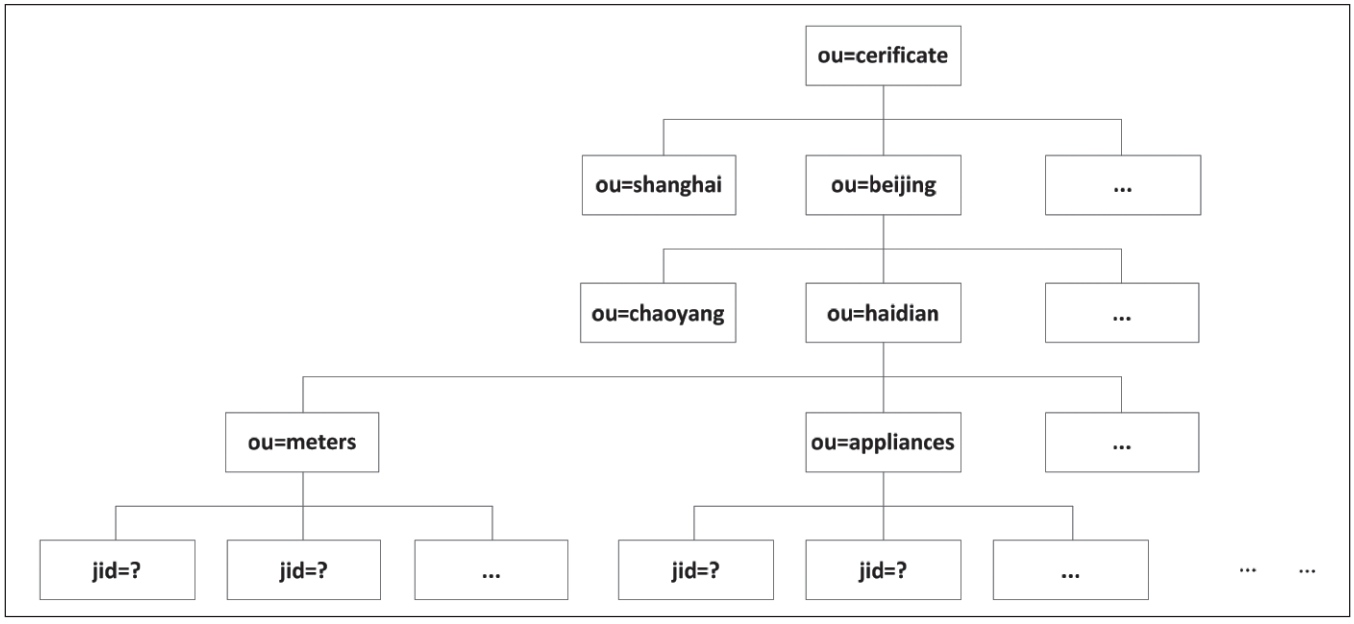

Fig.7 Diagram certificate catalog library DIT

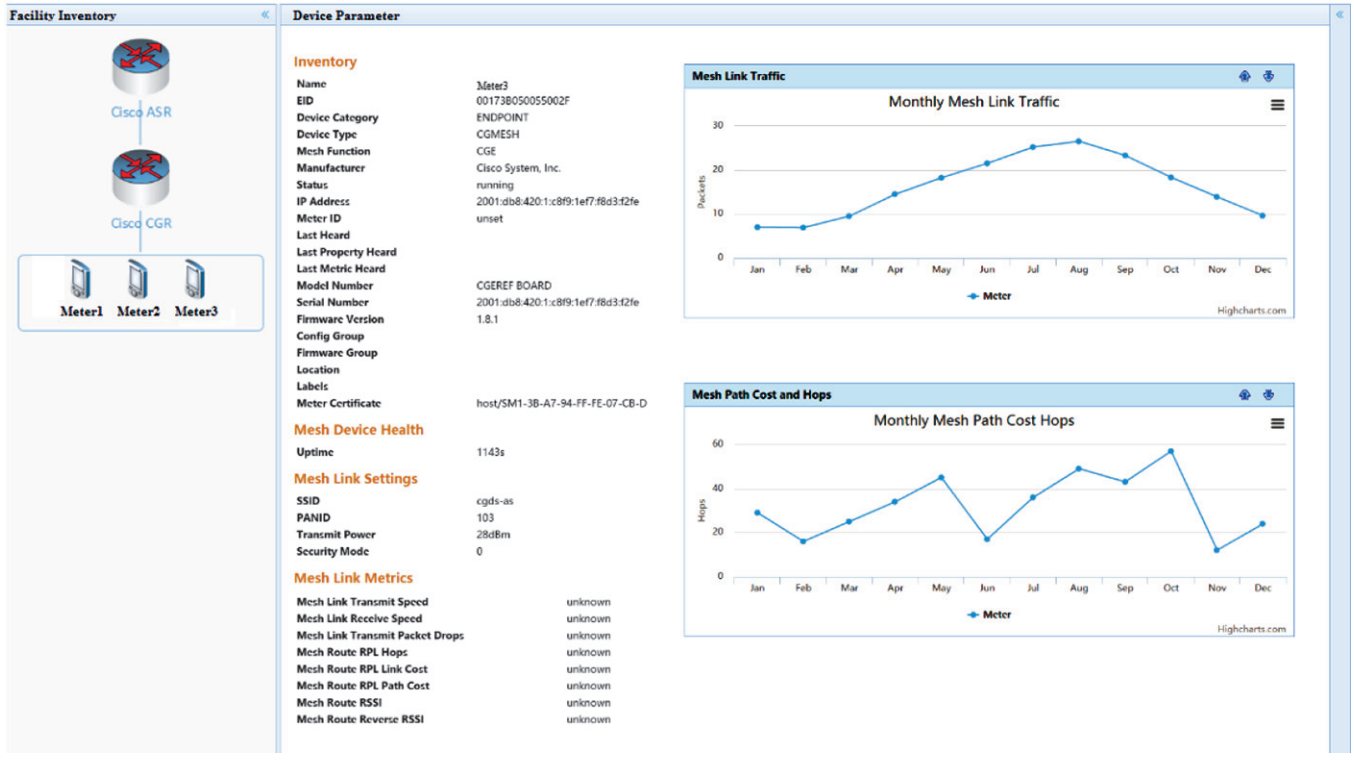

Fig.8 Result of the experiment

In this paper, the LDAP server of the SCEP protocol is designed, mainly for DIT tree design. The most important part of DIT tree is the branch that stores certificates and the CRLs. This branch provides adding, deleting, modifying certificates and CRLs for smart grid terminals. In the design of certificate branch, according to the regional division, the certificates of different regions are separately stored in different branch, so it is easy to find and management. Certificate catalog library DIT is shown in Fig.7.

3.3 Experiment Results

According to the design of AMI architecture based on IPv6 in this paper, we set up a real network environment. In this network, the front-end router is Cisco ASR 1001, the

convergence router is Cisco CGR 1120. This architecture can sense the smart meters when they access in and get out. What is more, it can sense the network topology. The results of the experiment are shown in Fig.8. The figure shows the network topology sensed by the AMI architecture, and the detailed information of smart grid meter, include the access time, mesh link traffic, mesh path cost and hops, etc. The experiment results show that, the new AMI architecture and the new authentication protocol could sense new smart meters which try to access to the smart grid.

4. Conclusions

In this paper, the process of the development of AMI in smart grid and its existing basic architecture are introduced. The smart meters, which are very important parts of AMI, are emphatically introduced. The AMI security requirements and the existing threats, especially in the aspects of security and privacy protection are analyzed. The new authentication protocol which uses SCEP to replace the existing EAP in IEEE 802.1x is proposed after the discussion of the special safety requirements of AMI. The new AMI architecture based on IPv6 is proposed which is applied in the proposed authentication protocol and the security authentication processes are discussed in detail.

5. Conflict of interest

This article content has no conflict of interest.

6. Referencs

[1] Y. Yan, Y. Qian, H. Sharif and D. Tipper (2013): "A Survey on Smart Grid Communications Infrastructures: Motivations, Requirements and Challenges", *IEEE Communications Surveys and Tutorials,* Vol. 15, No. 1, pp. 5-20, First Quarter.

[2] Lo, Chun Hao and N. Ansari (2012): "The Progressive Smart Grid System from Both Power and Communications Aspects", *IEEE Communications Surveys & Tutorials,* Vol. 14, No.99, pp. 1-23, 2012.

[3] F.M. Cleveland (2008): "Cyber security issues for Advanced Metering Infrasttructure (AMI)", 2008 IEEE International Conference on Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, No. 2008, pp.S1–S2.

[4] N. Liu, J. Chen, W. Liu and H. Luo (2011): "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure", Proceedings of 2010 the 3rd International Conference on Computational Intelligence and Industrial Application, Vol.2, No.2011, pp. 430-438..

[5] S. Azghandi, K. M. Hopkinson and RJ. Mctasney (2014): "An empirical model for smart meters using data security", 2014 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1-5.

[6] M. A. Faisal, Z. Aung, J. R. Williams and A Sanchez (2015): "Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study", *IEEE Systems Journal*, Vol. 9, No. 1, pp.31-44.

[7] H. Nicanfar, P. Jokar, K, Beznosov and VCM. Leung (20134): "Efficient Authentication and Key Management Mechanisms for Smart Grid Communications", *IEEE Systems Journal*, Vol.111, No.11, pp.2326–2337.

[8] D. Culler (1012); "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", 2012 6th International Conference on IEEE Signal Processing and Communication Systems (ICSPCS), Vol. 11, pp.1 - 6.

[9] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu and X. Shen (2011): "A Lightweight Message Authentication Scheme for Smart Grid Communications", *IEEE Transactions on Smart Grid*, Vol.2, No.4, pp. 675-685.

[10] S. Chatterjee, D. Sarddar, J. Saha, S. Banerjee, A. Mondal, et al.(2012): "An improved mobility management technique for IEEE 802.11 based WLAN by predicting the direction of the mobile node", 2012 National Conference on IEEE Computing and Communication Systems (NCCCS), pp.1-5.

[11] J. Zhou, R. Q. Hu and Y. Qian (2012): "Scalable Distributed Communication Architectures to Support Advanced Metering Infrastructure in Smart Grid", *IEEE Transactions on Parallel & Distributed Systems*, Vol. 23, No. 9, pp. 1632-1642.

[12] H. Hu, D. Kaleshi (2015): A. Doufexi and L. Li, "Performance Analysis of IEEE 802.11af Standard Based Neighborhood Area Network for Smart Grid Applications", 2015 81st IEEE International Conference on Vehicular Technology Conference (VTC Spring).

[13] K. Y. Park, S. K. Yong and J. Kim (2012): "Security enhanced IEEE 802.1x authentication method for WLAN mobile router", 2012 14th International Conference on. IEEE Advanced Communication Technology (ICACT), pp.549-553.

[14] K. H. Chi, Y. C. Shih, H. H. Liu and J. T. Wang (2011): "Fast Handoff in Secure IEEE 802.11s Mesh Networks", *IEEE Transactions on Vehicular Technology,* Vol. 60, No. 1, pp. 219-232.

[15] J. Kim, D. Kim, K. W. Lim, Y. B. Ko and S. Y. Lee (2012): "Improving the Reliability of IEEE 802.11s Based Wireless Mesh Networks for Smart Grid Systems", *Journal of Communications & Networks,* Vol. 14, No. 6, pp. 629-639, 2012.

[16] P. Balakris, K. Rajagopal and K. S. Swarup (2015): "Analysis on AMI system requirements for effective convergence of distribution automation and AMI systems", 2014 6th IEEE International Conference on Power India International Conference (PIICON).

[17] R. K. Bhatia and V. Bodade (2014): "Defining the framework for wireless-AMI security in smart grid", 2014 International Conference on IEEE Green Computing Communication and Electrical Engineering (ICGCCEE), pp.1-5.

[18] R. Vijayana, D. Devaraj and B. Kannapiran (2014): "A novel dual euclidean algorithm for secure data transmission in smart grid system", 2014 IEEE International Conference on IEEE Computational Intelligence and Computing Research (ICCIC).

[19] S. H. Seo, X. Ding and E. Bertino (2013): "Encryption key management for secure communication in smart advanced metering infrastructures", 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 498-503, 2013.

[20] Y. Liu, C. Cheng, T. Gu and T. Jiang (2015): "A Lightweight Authenticated Communication Scheme for Smart Grid", *IEEE Sensors Journal* , pp.1-.

[21] A. Lewandowski, V. Koster and C. Wietfeld (2010): "Performance Evaluation of AODV and OLSR-Meshed IP-Enabled IEEE802.15.4", International Conference on IEEE Advances in Mesh Networks, pp. 7-12.

[22] J. M. Chang, T. Y. Chi. H. Y. Yang and H. C. Chao (2010): "The 6LoWPAN Ad-Hoc On Demand Distance Vector Routing with multi-path scheme", Iet Digital Library, pp.204-209, 2010.

[23] C. J. Tang and M. R. Dai (2010): "An Evaluation on Sensor Network Technologies for AMI Associated Mudslide Warning System", 2013 International Conference on Computing, Networking and Communications (ICNC) IEEE, pp. 237-242.

FAILURE MECHANISM AND VIBRATION CONTROL FOR TOWER TUBE OF WIND GENERATOR UNDER EXTREME CLIMATE

(Continued from page 123)

[7] Guangling, Tian Jingkui, Chang Desheng (2013): Offshore wind turbine anti typhoon concept design of [J]. *Electric Power Construction*. (2): 11-17.

[8] Wu Jincheng, Zhang Rongyan, Zhang Xiuzhi (2010): Anti-typhoon design of offshore wind turbines [J]. *China Engineering Science*, 12 (11): 25-31.

[9] Prowell I Veletzos. M Elgamal et al (2009): Experimental and numerical seismic response of a 65 kW wind turbine steel tower [J]. *Journal of Earthquake Engineering,* 13(8):1172.

[10] Zhang Xiangting (1990): Wind load theory of engineering structure and wind resistant calculation manual [M]. Tongji University press.

[11] Zhang Peixin(2013): Building structure and wind load [M]. Shanghai science and Technology Publishing House.