Improvement of Home Appliance Control System in Smart Home Based on 6LoWPAN

Wei Fu
Key lab of industrial wireless network and networked control, Ministry of Education, Chongqing University of Posts and Telecommunications, Chongqing, China
Email: 40736286@qq.com

Gang Chen, Ping Wang, Yang Hong, and Houyang Ge
Key lab of industrial wireless network and networked control, Ministry of Education, Chongqing University of Posts and Telecommunications, Chongqing, China
Email: 920533962@qq.com, 962138164@qq.com

***Abstract*—Based on the developing requirement of digitalization, networking, and intellectualization in smart home, an improved scheme of home appliance control system is proposed in this paper. It is focused on the system identification and information security. The software designed for smart phone and PDA based on Android operation system is completed, the website based on architecture of J2EE is also developed .With the 6LoWPAN protocol based on IPv6 for WSNs, through the way of connecting to environment monitoring system, security guard and alarm system, this system can realize the function for the situational mode control, and also provide safe and full service for data exchanging to optimize people's life style.**

***Index Terms*—Smart home, Home appliance control, 6LoWPAN protocol, Android intelligent terminal**

I. Introduction

Smart home is based on a variety of home appliances. It combines network communication, information appliance, equipment automation, etc. It integrates system, structure, service, and management into a safe, high-performance, and convenient living environment [1]. With the high development of the Internet of Things and information appliance, more and more families are pursuing a more convenient lifestyle.

WSN (wireless sensor network) is a hot and multi-discipline research area in recent years. It synthesizes sensor technology, embedded computation technology, wireless communication technology, which has functions of real-time monitoring, detecting and collecting different environment information by the method of forming WPAN (Wireless Personal Area Network) with all kinds of integrated micro-sensors. Because of IPv6 has the characteristic of large space address, automatic address allocation, neighbor discovery and so on, it is ideal to be the network layer of WPAN. The combination of WSN and IPv6 will open new times of ubiquitous network [2]. The wide use of TCP/IP protocol makes it to be the actual standard of wired network. At the same time, the TCP/IP protocol is applied to wireless communication areas step by step. Hence, it is one of the pivotal WSN problems that should be solved to realize WSN and IP network communicate with each other. In 2004, IETF has established 6LoWPAN Working Group to solve the fusion problems of WSN and IPv6. The purpose of this group is to realize the seamless interconnection of WSN and IP network [3]. Using 6LoWPAN for Home Appliance Control System is reliable and safe.

By the way of using home appliances controller, smart home gateway to connect home appliances to WAN (Wide Area Network) such as Ethernet, Wi-Fi, GSM or 3G. It is realized the dream of controlling the information appliance anywhere and anytime.

II. Disadvantages of Existing Home Appliance Control System

A. Facing Some Barriers of using Variety of Wireless IOT Protocol to Communicate with Each Other Smoothly

Common home appliances such as induction cooker, electric cooker and fanner have not designed the communication interface for remote control [4]. It makes family users can't control this kind of home appliance with intelligent mobile phone, PDA, or visiting websites.

Almost all of home appliance remote controllers adopt infrared communication technology, because of the weakness of permeating opacity object, it is impossible to control these home appliance remotely that just using infrared technology.

B. Lack of Mechanism for System Identification and Information Security

At present, smart home is facing all kinds of network attacks, such as wiretapping signal, modifying network data packet, sending attack data packet, acquiring encryption algorithm by collecting the data that being transported on the network. The deficient mechanism for system identification and information security gives the

doi:10.4304/jcp.9.1.183-188

attackers the chance to make serious consequence that the system is controlled by them.

C. The Weakness of Multi- terminal Remote Network Control and Communication Ability

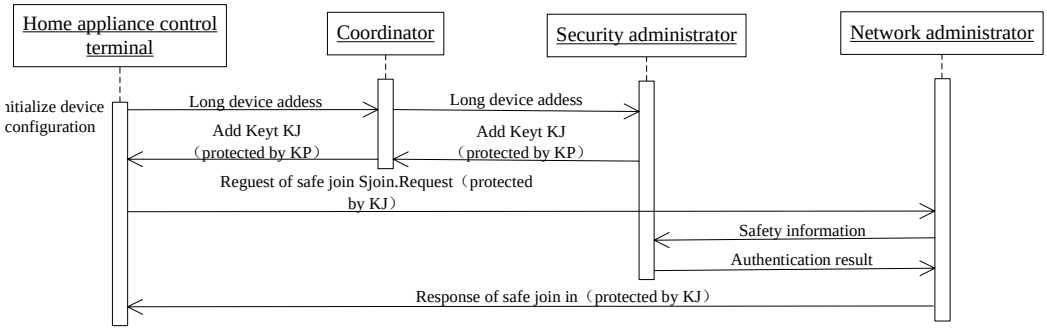

Figure 1. The schematic diagram of home appliance terminal joins in network safely.

The development of smart home is still in its infancy in China. There is a long way to go for the popularity of information appliance. At the moment, home appliances, which are widely used in daily life, have the weakness of too few communication interfaces to network smoothly. The users have to use matched remote controller to control corresponding home appliance at home. It is impossible for them to control home appliance and monitor indoor environment with mobile phone, PDA or website.

III. IMPROVEMENT OF THE SYSTEM

A. Protocol Conversion Technology

Home Appliance control system transmits messages through the TCP / IP protocol, sends messages to local home appliances WSN network, then the appliance control terminal will receive the information that transmitted by smart home gateway. The appliance control terminal parses command packets and makes the corresponding control of home appliances.

B. Identification &Information Security

To prevent some unauthorized users to malicious manipulate family appliances, avoiding the personal injury and property damage to legal users, the System need to check the user's identity to prevent non-professionals change network configuration parameters. Encryption includes symmetric encryption, asymmetric encryption, can be used in the appliance control system authentication, digital signatures and other information exchange occasions.

Based on the existing standards security of WSN and the security needs of smart home, it is necessary to make safe circumstance of smart home in multi-protocol environment and the limitation of the process capacity of equipment, we can solve access network security, messaging security, identification security between legitimate equipment and user access process control security from the aspect of access network security and data security.

1. *Access Network Security*

(1) Access Network authentication mechanism

Shown as Fig.1, access network authentication mechanism used to guarantee the authenticity of the terminal identity, which is an important part of network security. The system uses star or tree topology, the access network certification process includes the following 3 steps.

Step1: Before a new device joins in the network, the coordinator read 64 address of the new equipment and sends the address to the security administrator, security administrator produces join key KJ, and the key will be written in the new appliance control terminal through the coordinator.

Step2: The new equipment that has KJ continued to monitor the available channels within the network, the selected routing device or gateway device, using AES in CCM mode to generate network authentication code MIC-4 and constructed the join network request message Sjoin.Request, then sent to the corresponding routing or gateway.

$$MIC\text{-}4 = AES\_CCM\_Auth\ (EUI\text{-}64, Rand\text{-}128, KJ) \quad (1)$$

$$Sjoin.Request = E\ \{KJ, EUI\text{-}64 \mid Rand\text{-}128 \mid MIC\text{-}4\} \quad (2)$$

Where: EUI-64 is the device 64 bit global unique addresses, Rand-128 is generated 128 bit random code for the device.

Step3: After the network administrator receives a join security request, decrypts Sjoin.Request to acquire access network information, and transmits authentication to the security administrator. Based on network information Security administrators recalculated MIC-4 to verify the correctness of MIC-4. If valid, the network administrator will send response to the new device for joining in.

(2) Distributed access control mechanism based on controlled object

When external user controls the system, some invalid or unauthorized malicious may access to sensitive information, correspondingly, access control mechanisms can be used to solve this problem. This paper proposed use the distributed access control mechanism based on controlled object to ensure the system security controls, and also to minimize the overhead of terminal equipment at the same time.

There are two problems in centralized access control completely by community server. Firstly, the high security demands for the management center. Secondly, the heavy burden of Management Center will reduce the

efficiency of the system. What's more, single node control mode also faces two problems: the node energy consumption is too much, and the vulnerability of the nodes increases the threats of the system. Therefore, this paper proposed to use distributed control mode, and user accessing is controlled by smart home gateway, and user authority is controlled by node, as shown in Fig.2.

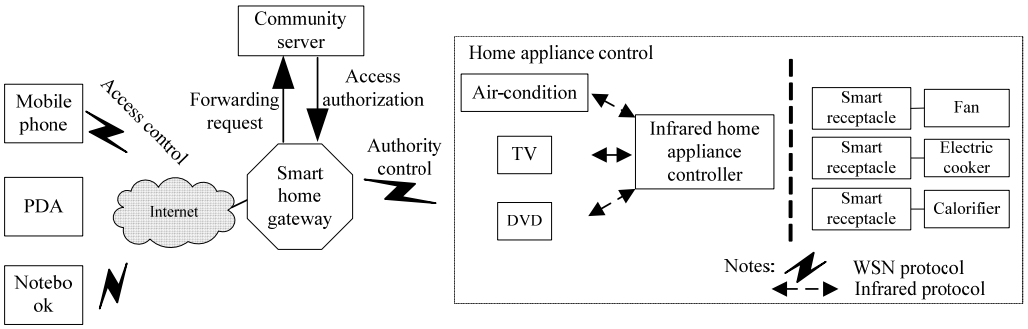

Figure 2. The network model of distributed access control

Community server is responsible for the formulation of control strategy, give out authorization when the user access and permission information to the appliance control terminal through smart home gateway, gateway and node stored user information and complete the access control over the user based on the stored information. After the user accessed safely, access control is adopted the symmetric encryption system to protect the security of information transmission. In this distributed control mode, the system can take a different password strategy based on the performance of different device. It is not only protecting the security of the system, but also reduces the node energy consumption.

(3) The anti-aggressive under the malicious access

Malicious behavior of access to smart home generally include replay attacks and DOS attacks, the aim of replay attacks is to obtain network access, the DOS attack is to paralyze the server or smart home gateway so that other legal users can't operate the system. In order to reduce the threat posed by such attack, this paper adds a timestamp in the packets of interaction of users, and use transmission delay real-time analysis in the system, using the user real-time traffic analysis and dynamically generate the relevant threshold approach. After access to the general user's propagation delay, the system dynamically generated threshold and configuration in the sensor network. The replay attacks judgment: the same user-network packet + (Tsend - Treceive > Tthreshold).After the analysis of user access flow under normal circumstances, the system dynamically generates N threshold (the maximum allowable number of requests per unit time), if received requests in unit time is larger than this value, we can judge that it is DOS attacks. The advantage of this method is:

1) system can change the time threshold dynamically to reduce the false rate of replay attacks, according to the real-time network transmission delay;

2) system can handle user's requests, limit user's access speed based on the current processing capability in the case of large traffic flow.

2.Data Security

(1) Centralized key management

Because of the number of control terminal is small in smart home. The scheme of centralized key management is adopted in this project. The appliance control terminal and the security administrator share the key. The key is generated uniformly by security administrator and being updated by the way of issuing. The basic key includes adding keys, key encryption keys and data encryption key, and on this basis, the key can go further expand according to its using situation.

①┌Key type

Join Key (KJ): It is a temporary key that used in the appliance control when terminals join in the network. Join key is generated in the phase of initialize device configuration, and distributed by the security administrator through the coordinator. Together with the long address of the equipment and join key generate the security information for authentication of the device. Join keys is used for secure distribution of KEK after equipment safely access to the network.

Key Encryption Key (KEK): It is the key that used for the encryption of a key when the key is in transmission. It is distributed by the security administrator. Security administrator distribute the KEK using join keys KJ to encrypt KEK at the first time; then using KEK to encrypt the new KEK to realize the secure distribution.

Data Encryption Key (KED): It is the key that used for the data protection and integrity checking in the data link layer and application layer. It is distributed by security administrators. Security administrators use the KEK to encrypt the KED to realize secure distribution.

②┌Key generation algorithm

Key generation intends to adopt SKG protocol which uses HMAC algorithm, HMAC algorithm schematic diagram is shown in Figure.3, ipad stands for the string of 16 hexadecimal value 0x36; opad stands for the string of 16 hexadecimal value 0x5C; stands for XOR operation; "||" stands for the connection operation; MMO Hash algorithm is none key hash algorithm, which is realized with the help of AES encryption algorithm.

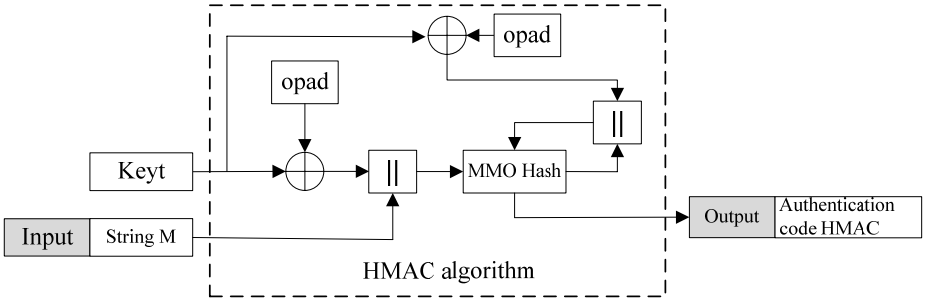

Figure 3. The principle diagram of HMAC algorithm

IV. System Design

A. System Topology

Home Appliance control system transmits messages through the TCP / IP protocol, sends messages to local home appliances WSN network, then the appliance control terminal will receive the information that transmitted by smart home gateway. The appliance control terminal parses command packets and makes the corresponding control of home appliances.

Fig.4 shows the topology of home appliance control system, user can access to the system by notebook, PDA or mobile phone. The server in the community stores the current state information of the system, and it is responsible for user identity and history logs. The community server transponds the control and query information from valid users to Smart Home Gateway, and the gateway sends parsed messages to the corresponding appliance terminal through WSN. The appliance terminals include infrared home appliance controller and smart receptacle.

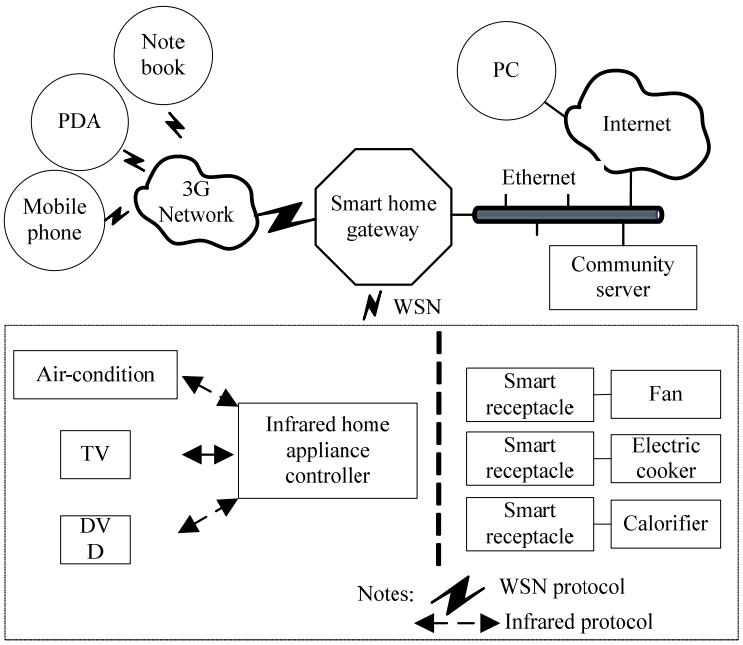

Figure 4. The topology of home appliance control system

B. WSN Protocol : 6LoWPAN

6LoWPAN has defined minimize TCP/IPv6 protocol for each senor node that enables IP communication for a single node like a computer, realizes seamless service between WSN and IP network, and ensures end-to-end communication on the Internet, it is important for WSN remote node control based on the Internet [5].

In order to network a low power consumption, dynamical, steady and remote transmission WSN, this paper networks WSN by using 6LoWPAN protocol, 6LoWPAN devices work in 2.4GHz with the characteristics of short range, low power consumption and low cost, and it uses the wireless Ad Hoc networks which has no restrictions on the number of equipment, a new nodes will be discovered automatically that improves the reliability of the network.

C.Software Design

1.Definition of application layer communication frame format

Stateless address auto-configuration is necessary for the 6LoWPAN network. The process requires interface ID of IEEE 802.15.4 MAC address at first, then configure

IPv6 address based on broadcast frame network prefix of router automatically. IPv6 address consists of 64 bit network prefix and 64 bit interface ID. The interface ID is generated by MAC address [6]. In the IEEE standard 802.15.4, MAC address can be either 64 bit long address or 16 bit short address. That is to say, IEEE standard 802.15.4 has 2 type of address: EUI-64 long address and 16 bit short address. For the EUI-64 long address, interface ID can be obtained from it directly. But for the 16 bit short address, it need be mapped to 48 bit dummy address first. Then it will be further mapped to EUI-64 long address and interface ID.

For the network communicates orderly, application layer communication frame format should be concise and accord with the requirement of system expansibility. The system retrenches the header of IPv6, compressing 128 bit address into 16 bit short address [7]. We use the adaptation layer to recover the compressed application layer header.

2.Community server

Server provides user cipher verification, operation permission matching, service integration, equipment adaptation, additional secret key, daily log management, etc. Server can encrypt important information using AES algorithm.

3. Mobile phone, PDA, website accessing

Fig.5 shows the control interface for Android smart phone [8]. Fig.6-- Fig.8 show control interface of web site based on J2EE. It is easy to use software to control home appliance such as air-condition, TV, light, fan, etc.

Figure 5. Interface for android smart phone

Figure 6. System login page

Figure 7. Air-condition control page

Figure 8. TV control page

V. Conclusion

The paper analyses the shortages of the existing home appliance control system, puts forward the improvement scheme of the protocol translation, identification, information security and remote control, and has taken further research in identification, information security. This paper puts the improved solution of the system based on 6LoWPAN. The system has realized two kinds of remote control methods, which based on Android smart phone and web site based on J2EE, for controlling air-condition, TV, fan and light, etc. And the system also provides communication interface to connect with other 6LoWPAN subsystem such as environmental monitoring and home security. Through the practical operation, it is demonstrated that the improved system works steadily, securely and efficiently. The system meets the requirement of real-time and unblocked.

Acknowledgment

This work is financially supported by the 2012 Annual Science and Technology Research Project of Chongqing Education Administration (No.KJ120534), Popular science series of Internet of things (cstc2012gg-kp1B40006), Internet of things the interactive experience on the research and development of library science exhibits and teaching aids (cstc2012gg-kp1B40005), in China. And Special Thanks to all who have helped to make this study.

References

[1] Yi Zhang, Junyuan Ma, Xiaoquan Yang, 2012, “Design and implement of Smart Home gateway based on Cortex and ZigBee”, TV Technology, 2012, 36(1) , pp. 56-57.

[2] Dae In Choi, Jong-tak Park, Su Yeon Kim, 2011, “Improve IPv6 Global Connectivity for 6LoWPAN”, 2011 13th International Conference on Advanced Communication Technology, pp. 1008- 1009.
[3] Han Ming, Miao Changyun, 2011, “The Design of Intelligent Household System Based on Wireless Communications”, 2011 International Symposium on Computer Science and Society, pp. 206-208.
[4] Rahmat Sanudin, Yoo Tuck Mun, Wan Suhaimizan, 2009, “Wireless Appliance Control System”, 2009 Conference on Innovative Technologies in Intelligent Systems and Industrial Applications, pp. 476- 478.
[5] Kim, J. Haw, R.Cho, E, 2007, “A 6LoWPAN Sensor Node Mobility Scheme Based on Proxy Mobile IPv6”, IEEE TRANSACTIONS ON MOBILE COMPUTING, vol. 6, No. 1, pp. 5- 7.
[6] Dhananjay Singh, U.S. Tiwary, Hoon-Jae Lee, 2011, “Global Healthcare Monitoring System using 6lowpan Networks”, International Conference on Advanced Communication Technology, pp. 114- 115.
[7] Yannis Mazzer, Bernard Tourancheau, 2009, “Comparisons of 6LoWPAN Implementations on Wireless Sensor Networks”, International Conference on Sensor Technologies and Applications, pp. 689- 690.
[8] Zhiqiang Wei, Qingchao Shi, Dongning Jia, 2012, “Design and Implementation of an Intelligent Information Integration System Based on Android Mobile Terminals”, International Conference on Computer Science and Electronics Engineering, pp. 162- 163.

Wei Fu was born in Lu Zhou city in Sichuan province in October 1981. She has received her control theory and control engineering master degree in Chongqing University of Posts and Telecommunication in China in June 2008, and received her electro-engineering bachelor degree in Sichuan Normal University in China in June 2005.

She is working in the Key Lab of Industrial Wireless Network and Networked Control, Ministry of Education in Chongqing, China, since July 2008, and now she is a lecturer and works in the field of network control in automation. She was the third inventor of the patent of invention of EPA field controller based on SOPC, She has published a textbook named electronic technology foundation as the chief editor (Chongqing, China: Beihang University Press, 2011,) and a monograph named high availability automation network as subeditor (Chongqing, China: Science Press,2011). And she now mainly researches in the Smart Home of the Internet of Things.

Teacher Fu had owned the second in the Chongqing Science and Technology Progress Award in 2009 for the key technology and application of EAP in the field control network.

Gang Chen was born in Neijiang city in Sichuan province in September 1987. He has received his Electric engineering bachelor’s degree in Sichuan Normal University in China in June 2010.

Now he is studying in the Chongqing University of Posts and Telecommunications, Chongqing, China, for a master degree since September 2010. he majors in control engineering. And he now mainly researches in the Smart Home of the Internet of Things.

Ping Wang received his bachelor’s and master’s degrees in in Chongqing University. He received his doctor’s degrees in Southwest Jiaotong University in China in June, 1994.

he is working in the Key Lab of Industrial Wireless Network and Networked Control, Ministry of Education in Chongqing, China, and now he is a professor and doctoral tutor. And mainly researches in the Internet of Things and Industrial Network Control Technology.

Yang Hong was born in Huainan city in Anhui province in December 1991.Now she is studying in the Chongqing University of Posts and Telecommunications, Chongqing, China, for a bachelor' s degree since September 2010.She majors in automation. And she now mainly researches in the elderly care system.

Houyang Ge was born in LuAn city in Anhui province in February 1991. He has received his Communication engineering bachelor’s degree in Sichuan University of South China in June 2012.

Now he is studying in the Chongqing University of Posts and Telecommunications, Chongqing, China, for a master degree since September 2012. He majors in control engineering. And he now mainly researches in the Smart Home of the Internet of Things.