Wireless Sensor Network, 2009, 1, 1-60
Published Online April 2009 in SciRes (http://www.SciRP.org/journal/wsn/).

The Analysis of the Structure and Security of Home Control Subnet*

Chengyi WANG[1], Yun ZHANG[2,3]
[1]*School of Electronic Engineering, Hubei University of Economics, Wuhan, China*
[2]*International School of Software, Wuhan University, Wuhan, China*
[3]*Research Center of Spatial Information and Digital Engineering, Wuhan University, Wuhan, China*
Email: wcytjx@126.com

Received November 16, 2008; *revised January* 10, 2009; *accepted February* 5, 2009

Abstract

A lot of technologies can be used in home control subnet, but the hardware and software resources available for the home control subnet are limited. There are security problems easily seen. The paper gives the systematic analysis of the structure and function of home control subnet based on the general model of home network. The paper has also analyzed two types of major equipment, namely sub-gateways and terminal equipment. The major networking technology used in home control subnet is summarized and concluded. In combination with relationship among home control subnet, home network, as well as the outside main network, the paper has systematically studied various safety problems related to home control gateways and the possible solutions to those problems have been made.

Keywords: Home Network, Home Control Subnet, Network Architecture, Network Security

1. Introduction

Home network is developed from the concept of home LAN, Intelligent home. It is the integrated networks of home control networks and multimedia information network, which is an integrated business platform with a voice, data, multimedia, video, control and management. Home network can be roughly divided into the high-speed backbone-network and low-speed control subnet. Subnet of control, there is a lot of technology and standards can be used, can be connected with home backbone-network, and even be connected with the Internet. Therefore, in building control network function, security issues associated with the network exists. The paper gives the analysis of the technology, structure and security issue of home subnet and also gives the description of the possible solutions.

2. The Architecture of the Home Control Subnet

2.1. The Reference Model of the Home Network Structure

Home control Subnet is one part of home network. It is described in detail in the structure reference model [1], as shown in Figure 1. The home backbone-network is linked with Internet and the management by home network gateway. Home control Subnet is connected with home backbone-network through sub-subnet gateway. Home backbone-network equipment can communicate with each other, getting access to external networks through the main gateway, holding the control operations of the equipment through the sub-subnet gateways. Home control subnet device can communicate through sub-gateway and the main gateway with the external home network.

2.2. Main Functions of the Control Subnet

The functions of home control subnet should be [2]:

- Inquiry function: the adoption of home control subnet gateway can query the status of subnet equipment;
- Control function: It can control the devices under the home control subnet through subnet gateways, but also implement the remote control through the main gateway;
- Configure function: implementation of the home sub-

*Fund Project: Hubei Province education department scientific research project (D200619006)

net configuration control operation;

- Message function: For auto-discovery, device management to provide basic information, it is able to take the initiative to send its status report to sub-gateways.

2.3. The Typical Structure of Home Control Subnet

A home network can have one or more home control subnet, each subnet network consisting of a subnet gateway and a number of terminal equipment. They can be connected through twisted pair, power line, radio frequency, infrared fiber and optical fiber, etc. One typical structure is shown in Figure 2.

2.4. The Structure of Subnet Gateway

Subnet gateway is one of the home control network equipment, whose functions are to enquire about the home control network device, parameter setting and control and to allocate and manage, home subnet equipment. In terms of hardware, sub-gateway is based on the 32-bit embedded system (such as the S3C2410x) to achieve implementation, shown in Figure 2. For the software, sub-gateways are based on embedded operating system (such as ARMlinux), Web server (such as boa), data base management system (such as SQLite) and so on to get the implementation.

As the central equipment of home control subnet, it is necessary for subnet to provide services for main network and external network, such as user authentication, remote control. It is needed for subnet to offer the service to the subnet equipment, such as the provision of the dynamic registration of terminal equipment, collecting the relevant data of terminal equipment. Subnet will also have the maintenance of a variety of information databases [3] and give sustained, reliable data information for information exchange and management. Its logical structure is as shown in Figure 3.

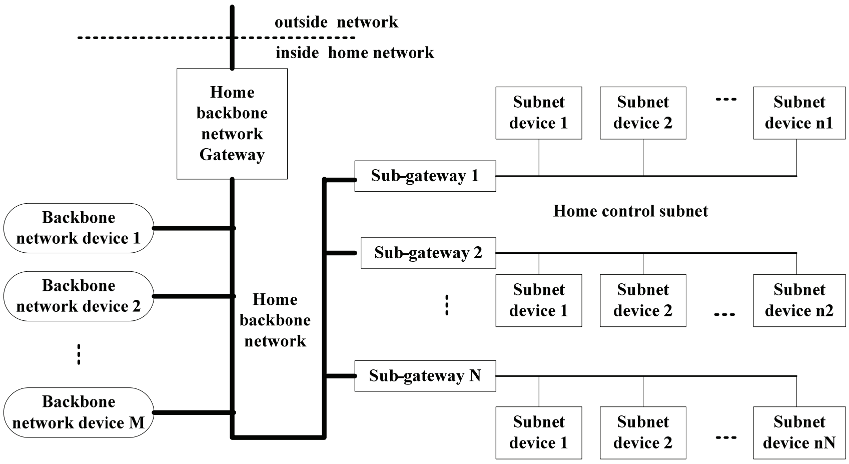

Figure 1. Home network structure reference model.

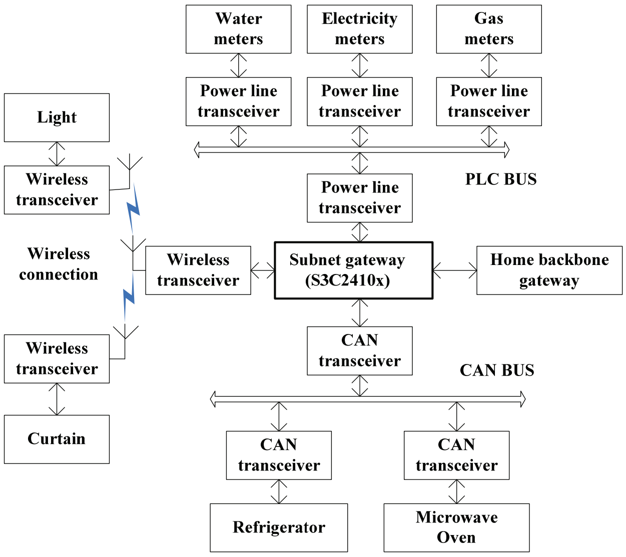

Figure 2. The typical structure of home control subnet.

Subnet gateway can provide remote services and remote control for the outside network user, the software architecture is as shown in Figure 4.

3. Networking Technology of Home Control Subnet

Home control subnet networking technology, according to the introduction of home network technology at the source, can be divided into bus technology, Ethernet technology and wireless network technology. Among them, the Ethernet technology mainly refers to industrial Ethernet technology. In terms of reliability, redundancy and other aspects of treatment improved the Ethernet technology is improved, but with less applications. Wireless network technology includes the 802.11 series, radio frequency, infrared, Bluetooth, ZigBee, etc. Bus technology can best bear the real-time control network, orderly and interoperable features. The typical of the bus technology is as shown in Table 1.

4. The Security Problems and Related Measures of Terminal Equipment and Wire

The Security risks of home control subnet may come from different levels, such as from the physics, the vulnerability of technology or man-made attack. The details are as follows.

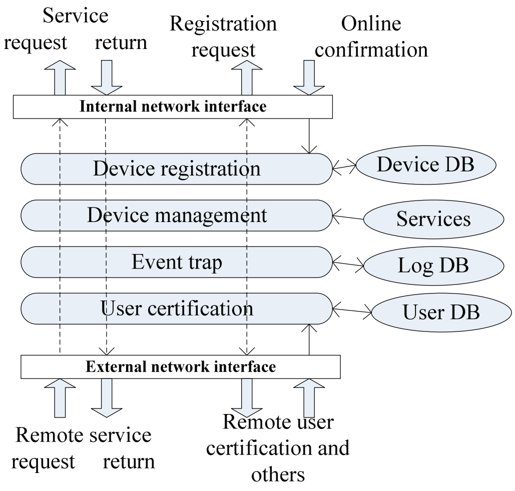

Figure 3. Subnet logical structure.

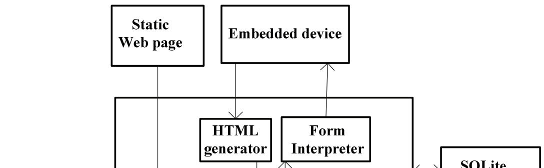

Figure 4. The subnet gateway software architecture.

Table 1. Typical bus technology.

Bus type	Relevant standards	The transmission medium	Maximum transfer rate
X-10	The standard in fact	power line	60bps
CEBus	ANSI IS-60/EIA-600	twisted pair, power line, coaxial cable, wireless	10kbps
LonWorks [4]	ANSI/EIA-709	Twisted pair, power line, coaxial cable, wireless and optical fiber	1.25Mbps
EIB	European Installation Bus Association	twisted pair, power line, wireless, infrared	10kbps
CAN [5]	ISO 11898-1	twisted pair, coaxial cable, and optical fiber	1Mbps

4.1. The Physical Security of Equipment

Problem 1: the physical security of equipment is the home control subnet gateway equipment, terminal equipment their own safety, including accident damage and man-made events, such as home gateways, connecting wires, home appliances equipment having been illegally linked, external electromagnetic interference, fire and other natural disasters.

Related measures: To set up password for access to essential equipment and more stringent measure of gateway certification is needed.

Problem 2: the power network security of the equipment and the security of weak power supply system.

Related measures: the use of effective protective circuit (such as the circuit with the energy absorption or photoelectric isolation function) for security.

Problem 3: There being more wireless networking technology in home control subnet, it may be overlapped with the frequency bands of other networks.

Related measures: the application of frequency bands approved by local relevant agencies for networking.

Problem 4: power line information security, including EMC (Electromagnetic Compatibility) and the signal separation.

Related measures: strict and effective grounding equipment, the use of isolators to isolate carrier.

4.2. The Protocol Security of Low Layer Network

Problem 5: RF wireless technology security, such as 802.11b technological security. Take 802.11b as an example, it shared key authentication by using one-way authentication method so that the access point can verify the identity of the user, but **users** can not verify the identity of the access point. If a false place is put to WLAN access points, it will hijack the legitimate client to launch a platform of DOS (denial of service stacks).

Related measures: By using two-way authentication mechanism so that detecting and isolating a false access point becomes possible. MAC address filtering, Wired Equivalent Privacy, etc. will be jointly used.

Problem 6: wireless coverage and information security. Neighbor device gets involved.

Related measures: One solution is to manually set ID for terminal equipment. The other is to verify the identity of terminal equipment.

5. The Security Problems and Related Measures of Subnet Gateway

As for the home control subnet, security of the gateway is most complex. In addition to the above mentioned similar device safety problems, more problems will occur at the top of network protocols. The security of subnet gateway is closely related with the location, structure and functions of subnet gateway. In terms of the location, the sub-gateway is key equipment between home control subnet and home backbone-network, being a member of the main network. In terms of the functions, the sub-gateways take the responsibilities of equipment registration, management and control, of verifying authentication of remote users, of information services and operational control. The sub-gateways for are responsible for the communication links between the main network and subnet, for the implementation of the centralized control and remote control of home control subnet terminal equipment, for bridging UPnP network upper protocol of main network. In terms of the protocol, the sub-gateways are involved in the multi-layered protocol stack. See Figure 5, showing that they result in different levels of network security problems.

The main security problems of subnet gateways are:

- Security of information: By the home sensors, an attacker can intercept domestic information of one family, such the working status of home appliances and personal privacy.
- User authentication: The attacker will illegally play as family members or staff of property management to read data and announce false instructions.
- User license: The attacker will illegal use or steal the authorization of the owner to take sabotage activities on purpose;
- Data integrity: An attacker will undermine the integrity of data through tampering the user's data and instructions. Specific analysis is as follows.

Problem 7: The safety of subnet gateway HTTP Authentication [6]. If the system is based on the HTTP basic authentication (Basic Authorization), and when the client makes requests to the HTTP server, HTTP server will determine the legality of the user through the basic certification process of verifying the client's name and password. In this certification process a user's name and password is submitted to the Web server after a 64-bit encoded files are put on the HTTP headers, but the password and user name is transmitted in plaintext way so that it can easily be intercepted and any user with that name and password can have access to these protected resources.

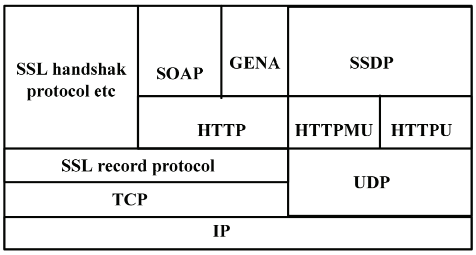

Figure 5. Subnet gateway protocol stack.

Related measures: For the weaknesses of basic authentication, HTTP/1.1 proposed to improve the user authentication program, known as the digest access authorization. With the similarity to the basic certification, digest access authorization is also a testing key know to both sides, but the transmission is not in plaintext way transmission, but in cipher text way transmission. Access control on the client can be divided into three steps, namely, identification authentication of clients and home gateway, the identification and authentication of client name and password, the check of the permissions of customer account.

Problem 8: How to encrypt and transmit important information.

Related measures: One solution is to use SSL (Secure Sockets Layer) protocol to simplify the information so that it applies to a subnet gateway of home network [7]. The protocol stack is as shown in Figure 5.

With the introduction of SSL protocol, it can upgrade the Web server and client communication confidentiality, data integrity and effective authentication. In combination with HTTP digest access authorization, different authentication can be done based on different levels of security. The visiting right is grouped. Through user groups of different terminals for different access control, and thus a more comprehensive security control can be achieved. The detailed measure is that different levels of equipment and its operation of home appliances will use different security systems. High security can hold SSL secure communication through the port of 443, or otherwise through the transfer port of 80 for HTTP, just use an easy authentication at the application layer. The main process of Web server is monitoring 80 ports and 433 ports. When 80 ports received request from HTTP, HTTP server would have digest access authorization to the clients. Upon completion of authentication, data will start to be transmitted. When there is a request of connection from the port of 443, the simplified SSL system which ensures security of transmission and authentication will be used.

Problem 9: Non-repudiation problem. It mainly refers to interaction between the two sides not denying the exchange of information, focusing on the user who cannot deny the operation on the home gateway and the terminal equipment.

Related measures: A basic approach is to log the user operations, to set up a log database. All users will be recorded for all operations. If the problem of non-repudiation is tackled, the adoption of digital signatures will matter.

Problem 10: Access Control security.

Related measures: For characteristics of home subnet, manager and user is usually the home member, therefore it is needless to grasp the complex set of internal details of permissions. As we know, there will be more types of electrical appliances at home their functions will become more and more complex. A possible solution is to establish the control strategy based on the object-model. From the perspective of the controlled object, the object-model will directly link the access to the subject with the controlled access object. On one hand, it is easy to operate the definition of the access control list object, deletion, addition and modification. On the other hand, when the controlled object feature changes, or the controlled object has the action of inherit and derivation, there is no need to update the access to the subject with the permissions, only need to modify the corresponding access of the controlled object, thereby reducing access to management of subject and decreasing the complexity of the authorized data management.

Problem 11: The security of device auto-discovery mechanism based on UPnP (Universal Plug and Play) [8] [9]. In order to get the intelligence of home backbone-network, there will be implementation of equipment, service auto-discovery protocol stack. The most typical one is UPnP. Because of malicious intrusion to the equipment, UPnP as the main equipment of home backbone-network, by subnet gateway as bridge, will get information of control subnet terminal equipment, and can do further attacks.

Related measures: the log can be used to record the user's operation, alarm. Subnet gateway can use the appropriate sub-gateway packet filtering strategy.

Problem 12: The security problem of virus attack and hacker attack.

Related Measures: The main solution is that the main gateway of home network is armed with firewall function so that it can block and prevent the attack of viruses, Trojans, hacker, and so on.

6. Conclusions

Through systematic analysis of the home control subnet structures, networking, and the relations of home control subnet and home backbone-network, especially the structure, functions of subnet gateway of home network and protocol stack, safety issues of home control subnet in different levels and aspects, including security of physical security equipment, the safety of the underlying protocol and the protocol level, are analyzed in detail and workable solutions are provided step by step. In short, as long as we make the full use of limited resources of the control subnet, make a reasonable choice of technology and build different levels of security precautions, a reliable and practical home control subnet will be surely constructed.

7. References

[1] SJ/T 11316-2005, "Home network system architecture and reference model," People's Republic of China Electronic Industry Standard, September 2005.

[2] SJ/T 11314-2005, "Specification for home subnet communication protocol," People's Republic of China Electronic Industry Standard, September 2005.

[3] SJ/T 11317-2005, "Home network device description file specification," People's Republic of China Electronic Industry Standard, September 2005.

[4] F. Q. Wu, J. Li, and D. S. Hu, "Application of LON works field bus technology in home network system," Journal of Chengde Petroleum College, Chengde, No. 4, pp. 31–56, 2008.

[5] Bosch, "CAN specification Version 2.0," September 1991.

[6] Y. Zhu, "Design and realization of an improved HTTP digest authentication scheme," Study on optical communication, Wuhan, No. 4, pp. 59–62, 2008.

[7] Y. Y. Zeng and Z. H. Zuo, "Design and implementation of SSL protocol on embedded devices," Journal of Chengdu University of Information Technology, Chengdu, No. 4, pp. 389–392, 2008.

[8] UPnP Forum, "UPnP device architecture 1.0," April 2008.

[9] SJ/T 11310-2005, "Information device intelligent grouping and resource sharing Part1: Core protocol," People's Republic of China Electronic Industry Standard, September 2005.