A Smart Home Network Simulation Testbed for Cybersecurity Experimentation

Jizhou Tong[1], Weiqing Sun[2(✉)], and Lingfeng Wang[1]

[1] Department of EECS, The University of Toledo, Ohio, USA
{jizhou.tong,lingfeng.wang}@utoledo.edu
[2] Department of ET, The University of Toledo, Ohio, USA
weiqing.sun@utoledo.edu

Abstract. With the rapid development of smart home, it becomes essential to study techniques to safeguard the home area network (HAN) against various security attacks. In this paper, a smart home network simulation testbed has been developed for security research in this area. It is designed to feature high fidelity, cost-effectiveness and user-friendliness. The testbed enables users to specify the HAN network topology, communication protocols and appliances, as well as develop security mechanisms such as information flow tracking. For the evaluation purpose, two security mechanisms were implemented on the testbed and their effectiveness against attacks is studied using the developed testbed.

Keywords: Smart Home Network Simulation Testbed · Home Area Network · Smart Home Security · Cyber Security

1 Introduction

With the development of the Smart Grid and sophisticated network technologies, it is possible that intelligent information services can be enabled in a household environment. Smart home provides high-quality services to the users by deploying smart devices in the home area network (HAN), through which the Smart Grid connects with the consumers. ZigBee is the most popular network protocol used in the HAN thus far, which is a specification for a suite of high level communication protocols used to create personal area networks built from small, low power digital radios [1], [2].

However, the problem of cyber security becomes more and more important as the home becomes smarter, because malicious attacks may bring a significant impact to the HAN environment. For instance, attackers may obtain the control authority of the smart home through a well-designed attack. Under this condition, he or she can control all the appliances in the home, which may cause more serious consequences such as changing the room temperature or increasing the electricity consumption. Although the ZigBee protocol provides some security mechanisms, it is not sufficient to meet the security requirements of the smart home network. And advanced network security mechanisms should be deployed in the smart home network. In order to evaluate these

V.C.M. Leung et al. (Eds.): TridentCom 2014, LNICST 137, pp. 136–145, 2014.
DOI: 10.1007/978-3-319-13326-3_14

security mechanisms effectively, a smart home network testbed needs to be created which can support the experimentation of HAN security mechanisms. However, it will be costly to build and maintain a real smart home environment; therefore, we aim at building a cost-effective simulation testbed in this study.

In this paper, a smart home network testbed simulation environment is created. Two security mechanisms are implemented in this testbed to show that it can support the research on the HAN security mechanisms.

2 Possible Attacks in the Smart Home Communication Environment

In the smart home communication network, four types of attacks may occur, including radio jamming attack, device impersonation attack, replay attack and non-repudiation attack.

2.1 Radio Jamming Attack

Radio jamming is the process of transmission of radio signals that disrupt communication by decreasing the signal to noise ratio. A radio jamming attack can cut off the communication or result in a very high latency between the sender and the receiver. During the data packet transmission, the packet will be damaged in a jammed communication medium before it is received. A jamming attack can be launched by transmitting a constant stream of data in the same channel. In a smart home communication environment, this type of attack can delay the communication between the smart meter and home appliances for a long period of time.

2.2 Device Impersonation Attack

In an HAN environment, some advanced malicious devices can bypass the authentication mechanism and obtain the right of communicating. Then, they may disguise as any device in the HAN, which can lead to malicious data being logged into the HAN communication environment. If the malicious devices disguise itself as the smart meter, it will get the control rights of the HAN and can send the malicious control commands to all the home appliances, which may lead to undesired consequences. For instance, some appliances can be shut down unusually or the load of some appliances can be set too high. Additionally, if the malicious devices disguise as the home appliance, it may send the malicious data to the smart meter, which may cause abnormal operations such as losing control to the home appliances, no response to some requests from the home appliances or the smart meter turned off abnormally.

2.3 Replay Attack

A replay attack is the network attack in which the same valid message is resent or delayed maliciously or fraudulently. This type of attack is usually launched by the third parties. In the HAN communication environment, the attacker can intercept the authentication information of home appliances with the smart meter through a

network monitoring tool. And then, the attacker can resend it to the smart meter. As a result, the attacker may invade the HAN successfully, which may cause the smart meter to overload. If the attacker launches the replay attack by controlling a home appliance, it may lead to the damage of the appliance by untimely activation.

2.4 Non-Repudiation Attack

Non-repudiation means that when a user uses or accepts one service, he or she cannot claim that the service is not used by him or her. In a smart grid communication environment, non-repudiation attack occurs when a customer denies using any service from the utility. In an HAN, the smart meter is controlled by the utility. The utility provides some necessary services to the HAN smart meter such as electricity real-time prices. The customer can deny the service of electricity real-time price in a smart meter by launching a non-repudiation attack, which may lead to economic losses for the utility companies.

3 Related Work

Previous research on the smart home simulator has been focused primarily on saving energy [3], [4]. A research to improve energy efficiency for smart building is presented in [5]. Some of them focus on the real home automation applications based on the sensors [6] and the method to create a test-bed for smart home [7], [8]. Some of the research work focuses on the smart home control systems [9], [10]. The machine to machine (M2M) network technology and its application in some areas such as healthcare and energy management are presented in [11] whose contribution is not only on the security issues of M2M network, but also on the quality of service and energy efficiency. Relatively little work has been done on how to create a smart home simulation platform for studying various security mechanisms in the HAN. Most of the current simulators for network simulation cannot meet the requirements for simulating a smart home environment with communication security mechanisms.

In [12], the authors carried out a research on several reality models to build a simulation platform for analyzing the network performances of the HAN. But, it primarily focuses on the network simulation of the HAN, and the security for the HAN is not considered in the study.

In [13], the authors present a multi-purpose scenario-based simulator for smart home. This simulator provides the ability to design the house plan and different virtual sensors and appliances. As a whole, this simulator can be good at simulating sensors and the appliances in the smart home. But the communication security is not considered in this smart home simulator.

In [14], the author presents a smart home simulation tool for energy consumption and production. This tool can give a graphical modeling platform of a smart home energy consumption based on the weather and energy price data input by the users. This simulation tool is good at simulating the energy consumption of a smart home. Nonetheless, as most of the smart home simulators, the network security mechanism in the smart home is not considered in the simulator.

4 Requirements of the Smart Home Network Simulation Testbed

Some key components are essential for building a smart home network simulation testbed for cybersecurity research. As shown in Fig. 1, there are four key components in a smart home environment, including the network module, control center module, home appliance module and security module. The control information is shown by green arrows and the status information is shown by yellow arrows. Control center can receive status information from home appliances and send proper control information to the appliances through the smart home network. The security module can secure the data transmission. The key design requirements and characteristics of the four modules are described later.

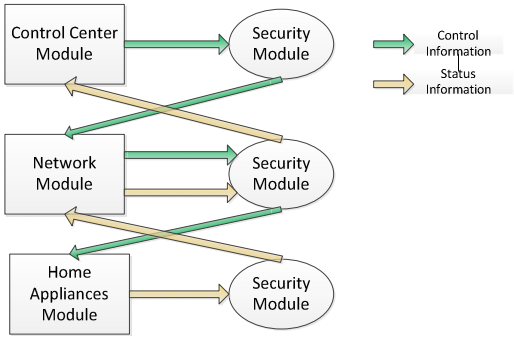

Fig. 1. Key Modules in Smart Home Network

4.1 Smart Home Network Module

The type of a smart home network can be wired or wireless. Wired communication is the fastest and most secure mode of the communication. But the cost for cabling and change in the existing structure of smart home needs to be considered. The wireless communication has an advantage over the wired communication since the wireless network is easy to install and configure in an HAN environment. The existing structure needs fewer modifications when the wireless communication is installed.

Various wireless technologies can be used for implementing a smart home network module such as Bluetooth, Wi-Fi (IEEE 802.11) and ZigBee (IEEE 802.15.4). From the comparison of these technologies, ZigBee is considered to be most suitable for the communication in the HAN of the smart grid. Because the master-slave architecture of Bluetooth has a limitation that only seven slaves can be added in a piconet, which is a constraint to the smart home network structure. The radio launched by Wi-Fi consumes a large amount of power. If Wi-Fi is used in the smart home network structure, batteries replacement in battery-operated home appliances may be required frequently. Compared with other wireless technologies, ZigBee provides a sufficient data rate for smart home network communication. Its radio consumes less power than other wireless technologies. In the simulation testbed, ZigBee protocol will be provided, and other communication technologies will be incorporated to fulfill the requirements of different users.

4.2 Control Center Module

The smart meter is the control center of an HAN environment, which is different from the traditional meter. The traditional meter in a house only collects the data of energy consumption of the home. There is no communication functionality in a traditional meter. For a smart meter, it can not only collect the energy consumption data of the whole house, but also indicate the energy consumption data of every home appliance. There are also some important network functions in the smart meter such as sending control commands to the home appliances, receiving the service information from the utility, collecting the feedback information from the home appliances in order to monitor their status, and providing the real-time electricity price to the customer. The communication between smart meter and home appliances is the single-hop communication. Because the smart meter needs to communicate with and control all the home appliances, the network type must be multi-channel.

4.3 Home Appliance Module

The biggest difference between home appliances in an HAN and traditional ones is that in an HAN they are controlled by the control commands sent from the smart meter through the home network environment. The traditional home appliances are controlled by using their switches. In a smart home, there may be no control switch on every home appliance. Instead, they are controlled by the smart meter through the HAN. Therefore, the network components of the sender and receiver need to be added to every home appliance in order to send their status to the smart meter and receive the control commands from the smart meter respectively. The type of the communication between every home appliance and the smart meter is single channel. The real-time status of the home appliances needs to be monitored by the smart meter. Some special home appliances like air-conditioners and heaters have multi-level power modes and can work under different modes. For these appliances, the smart meter can send different control commands to change their working modes.

4.4 Security Module

Network communication security is important to the smart home. In the testbed, a security module is designed so that users can develop their own security policies by using this module. The security module can have multiple security mechanisms, such as the information security checking mechanism and security label mechanism. These mechanisms can make the information flow secure during their transmission among the control center module, network module and home appliance module. The security module is embedded in all the other three modules. For instance, the control information will be checked by the security mechanisms of the security module before they are sent to the home appliance module through the network module. It will be sent after making sure that the data packet is legitimate.

5 Design and Implementation of the Smart Home Network Simulation Testbed

Based on the requirements of the simulation testbed, our simulator should be able to simulate the smart meter, various smart appliances and the HAN. Matlab/SimuLink provides a comprehensive tool to achieve the desired objective. It is able to simulate the power flow and communication flow in the smart home environment. For the communication network, TrueTime toolbox was used to facilitate the simulation of network protocols in a HAN. TrueTime is an add-on in Matlab/SimuLink, useful for real-time modeling of SimuLink models [15]. This toolbox facilitates co-simulation of controller task execution in real-time kernels network and transmission. It is developed in C++ language. One of its useful features lies in the network simulation including Ethernet, CAN, WLAN and ZigBee. Nonetheless, the TrueTime toolbox does not provide any security mechanism when a network control system is created. In order to facilitate the HAN security study, additional security models should be added on top of TrueTime toolbox. Based on TrueTime, smart home networks with user-specified configurations can be simulated.

5.1 The Structure of a Typical Smart Home Network

As seen from Fig. 2, there are ten appliances in the smart home. The smart meter is the smart control device, and other nine home appliances are controlled by the smart meter. The control commands are sent by the smart meter through the ZigBee network to the home appliances. After the control commands are received by the appliances, every appliance will give its energy usage information as a feedback to the smart meter through the ZigBee network so as to provide its current status.

Every appliance under control has three components: controller, actuator and sensor. These three components are logically independent with their appliance. They are embedded into each appliance. For every appliance, the control command is received by its controller. Then, the controller sends the control command to the actuator. After the actuator executes the command and changes the appliance status, the sensor sends the current status of the appliance back to the smart meter. The whole loop control process is shown in Fig. 3.

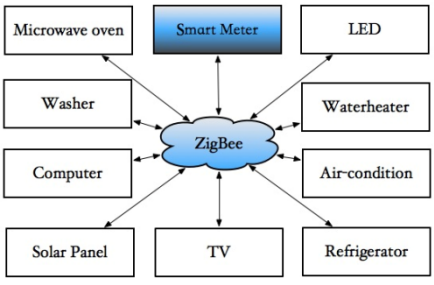

Fig. 2. Structure of a Typical Smart Home Network

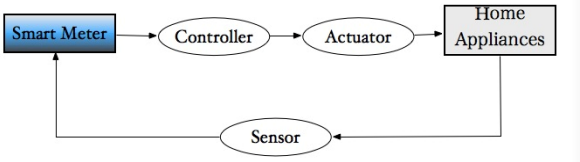

Fig. 3. The Process of Closed Loop Control

5.2 Smart Home Network Simulation Testbed Implementation

The testbed structure is shown in Fig. 4. Every block is a subsystem. The control center subsystem block simulates the functions of the smart meter which is the control center in the smart home. The ZigBee subsystem block is the TrueTime kernel network block which can simulate the wireless networks including 802.11 b/g (WLAN) and 802.15.4 (ZigBee).

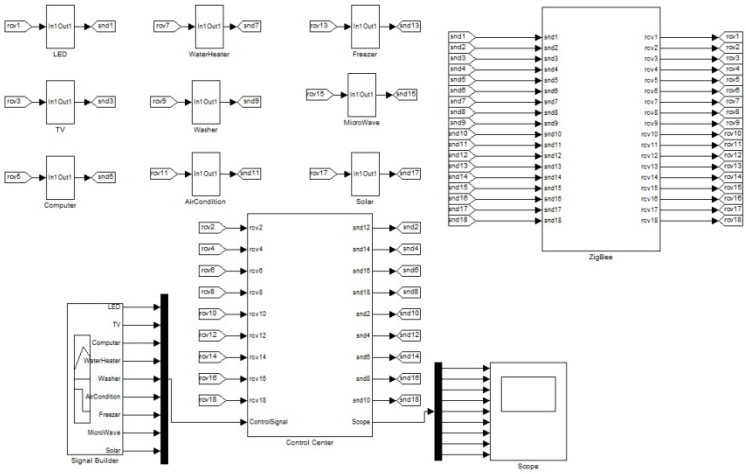

Fig. 4. Structure of the Smart Home Network Simulation Testbed

There are mainly two parts in the meter subsystem: one component sends control signals to the home appliances, while the other receives the energy usage feedback information from the home appliances. Meter subsystem uses nine TrueTime send blocks and TrueTime receive blocks to implement the function of sending control signals and receiving energy usage feedback information, respectively.

The TrueTime wireless network block is used in the ZigBee network subsystem. It provides two types of networks: ZigBee and WLAN. In this work, the ZigBee network is selected. Because the control signals sent to the nine home appliances and the energy usage feedback information received from the home appliances must go through the ZigBee network subsystem, the send port has 18 inputs and the receive port also has 18 outputs in this block.

For the home appliances subsystem, there are four types of blocks in the subsystem, which are TrueTime send block, TrueTime receive block, switch block and

constant block. The TrueTime send block sends the energy usage feedback information to the meter subsystem through ZigBee network subsystem. The TrueTime receive block receives the control signal sent by the meter subsystem. The constant block with a value 0 represents the power off status of the home appliance. Another constant block with a different value for different home appliances subsystem represents the power of the home appliance. The switch block is connected with other three types of blocks. The control signal received by the TrueTime receive block can change the status of home appliance through controlling the switch block. Fig. 5 shows a LED subsystem. The power of the LED is 0.015 KW.

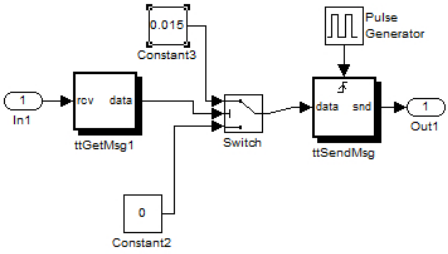

Fig. 5. LED Subsystem

5.3 Security Mechanism Implementation

Security mechanisms can be developed by the users based on the simulation testbed. Essentially, hook functions have been inserted into the network communication protocols. And users can develop code for those hook functions to implement their desired security mechanisms. The current testbed provides two such security mechanisms, which are information security checking mechanism and security label mechanism.

5.3.1 Information Security Checking Mechanism Implementation

Information security checking mechanism is designed to implement information flow control. In the smart home, the control information only can flow from the smart meter to the home appliances, and the feedback information can only flow from the home appliances to the smart meter.

The data type, source address and destination address will be checked before a message is sent or received in order to implement the information flow control presented above.

For example, the smart meter needs to send a control command to an appliance. For the sender, the data packet will be sent under the condition that the data type is control information, the destination address is a legal device and the source address is the control center. For the receiver, the data packet will be received under the condition that the data type is control information, the source address is the control center and the value of the destination address is correct.

From the process of the information security checking mechanism of the sender and receiver, the source address can be seen as sender ID; and the destination address can be seen as receiver ID. In order to implement the security checking mechanism, the legality of the sender and receiver ID must be checked in both of ttsend and ttreceive S-Function blocks in the smart meter block and home appliance blocks of the smart home network simulator. The sender ID, receiver ID and the number of nodes in the current network can be obtained by using pointers in the ttsend and ttreceive S-Function. If the values of the sender ID and receiver ID are less than the value of 0 or greater than the value of the number of nodes in the current network, they can be seen as illegal. And the ttsend and ttreceive S-Function will be terminated.

5.3.2 Security Label Mechanism Implementation

The security label mechanism is to add a security label field to the data packet before it is sent. The value of this label can be a string of characters defined by users, which make the data packet unique in the smart home network. Before the data packet is received, the receiver must check the security label of the data packet in order to ensure that the data packet belongs to the current network environment and the value of security label is correct.

A constant block called SecurityLabel has been added into the send block, which can be used to implement the security label mechanism. Under this condition, all the data packets sent by the send block of the smart home network will have a unique security label. For the receiver in this testbed, a security label checking function needs to be added into the ttreceive S-Function. For the process of the checking security label function, the value of the SecurityLabel is obtained through a pointer, and then the value is checked before the data packet is received. If the value of SecurityLabel field is equal to the specified value, the data packet will be received. If not, the data packet will be dropped.

6 Conclusions and Future Work

This paper presents a smart home network control system simulation testbed for studying HAN security mechanisms based on TrueTime toolbox. Two security mechanisms are provided in this simulator, which are information security checking mechanism and security label mechanism. The process of implementing the two security mechanisms demonstrated that this smart home network simulator can support the HAN security mechanisms effectively.

For the future work, more characteristics of the real home appliances will be implemented in the home appliances module. For example, some home appliances, including air-conditioners and heaters, have multiple energy consumption levels. In addition, a GUI will be designed to enhance the usability of the testbed. More security mechanisms will be implemented in this smart home network testbed, which can provide users more choices to conduct the research on the smart home network security.

References

1. Farahani, S.: ZigBee Wireless Networks and Transceivers. Newnes. pp. 1–3 (2008)
2. Guo, W., Healy, W.M., Zhou, M.: Interference Impacts on ZigBee-based Wireless Mesh Networks for Building Automation and Control. In: 2011 IEEE International Conference on Systems, Man, and Cybernetics, pp. 3452–3457 (2011)
3. Fensel, A., Tomic, S., Kumar, V., Stefanovic, M., Aleshin, S.V., Novikov, D.O.: SESAME-S: Semantic Smart Home System for Energy Efficiency. Informatik-Spektrum **36**(1), 46–57 (2012)
4. Jin, C.: A Smart Home Networking Simulation for Energy Saving. Carleton University (2011)
5. Louis, J.N.: Smart Buildings to Improve Energy Efficiency in the Residential Sector. University of Oulu (2012)
6. Gill, K., Yang, S.H., Yao, F., Lu, X.: A Zigbee-based Home Automation System. IEEE Trans. Consum. Electron **55**(2), 422–430 (2009)
7. Mekikis, P.V., Athanasiou, G., Fischione, C.: A Wireless Sensor Network Testbed for Event Detection in Smart Homes. In: 2013 IEEE International Conference on Distributed Computing in Sensor Systems, pp. 321–322 (2013)
8. Molitor, C., Benigni, A., Helmedag, A., Chen, K., Cali, D., Jahangiri, P., Muller, D., Monti, A.: Multiphysics Test Bed for Renewable Energy Systems in Smart Homes. IEEE Trans. Ind. Electron **60**(3), 1235–1248 (2013)
9. Perumal, T., Ramli, A., Leong, C.: Interoperability Framework for Smart Home Systems. IEEE Trans. Consum. Electron **57**(4), 1607–1611 (2011)
10. Suh, C., Ko, Y.B.: Design and Implementation of Intelligent Home Control Systems based on Active Sensor Networks. IEEE Trans. Consum. Electron **54**(3), 1177–1184 (2008)
11. Chen, M., Wan, J., Gonzalez, S., Liao, X., Leung, V.: A Survey of Recent Developments in Home M2M Networks. IEEE Communications Surveys and Tutorials (2013). doi:10.1109/SURV.2013.110113.00249
12. Liang, Y., Liu, P., Liu, J.: A Realities Model Simulation Platform of Wireless Home Area Network in Smart Grid. In: 2011 Asia-Pacific Power and Energy Engineering Conference, pp. 1–4 (2011)
13. Jahromi, Z.F., Rajabzadeh, A.: A Multi-Purpose Scenario-based Simulator for Smart House Environments. In: (IJCSIS) International Journal of Computer Science and Information Security, vol. 9, no. 1, pp. 13–18 (2011)
14. Krzyska, C.: Smart House Simulation Tool, Master thesis, Informatics and Mathematical Modelling, Technical University of Denmark, DTU (2006)
15. Cervin, A., Henriksson, D., Ohlin, M.: TRUETIME 2.0 beta - reference manual. Lund University (2010)