Journal of Computer and Communications, 2014, 2, 1-7
Published Online May 2014 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2014.27001

Scientific Research

Design and Implementation of Secure Nodes in the Based-Internet-of-Things Intelligent Household

Xiangdong Hu, Hongru Xu, Kaimin Han

College of Automation, Chongqing University of Posts and Telecommunications, Chongqing, China
Email: huxd@cqput.edu.cn

Received January 2014

Abstract

As one of the most important uses of the Internet of things (IOT), the intelligent household is becoming more and more popular. There are many fragile nodes in the intelligent household and they are bound to encounter some potential risks of hostile attacks, such as eavesdropping, denial of service, error instructs, non-authorized access or fabrication and others. This paper presents a method of design and implement of secure nodes for the intelligent household based on the IOT technology, besides giving the hardware model of nodes, the management of key, the access authentication of network, the transmission of encrypted data, and the alarm based on intrusion detection and other security mechanisms. That is, to improve the security of the based-IOT intelligent household from the viewpoint of nodes security. A test platform is built and the results of simulation prove that the proposed method can effectively improve the security of the intelligent household from access safety and transmission security.

Keywords

The Intelligent Household, The Internet of Things, Secure Nodes, CC2530, Mechanism of Security

1. Introduction

As one of the emerging strategic high-tech industries in today's society, the Internet of things has already been listed into "the national five-year development plan outline of China", the research and application of the Internet of things technology is bound to accelerate the industrial upgrading and transformation, at the same time, to steadily promote the development of the national economy, to constantly enhance the comprehensive national strength [1]. The intelligent household is one of the most important applications of the Internet of things.

How to cite this paper: Hu, X.D., Xu, H.R. and Han, K.M. (2014) Design and Implementation of Secure Nodes in the Based-Internet-of-Things Intelligent Household. *Journal of Computer and Communications*, **2**, 1-7.
http://dx.doi.org/10.4236/jcc.2014.27001

In recent years, many cities in China have built a great number of intelligent infrastructures such as the intelligent buildings, the intelligent households, the intelligent communications, or the intelligent logistics. To gain a better quality of life, more and more people hope the house which they are living now to be intelligent and convenient. According to the report of the science and intelligent construction technology development promotion center of the national ministry of construction of China: Due to the advantages in environmental protection, health care, safety and comfort, the intelligent household have gradually become popular, the number of the intelligent household will increase sharply, the ratio of intelligent household is reaching around 20% now [2].

With the continuous development of the intelligent household, more and more kinds of sensors are used in the intelligent household, the number of nodes is increasing, too, any nodes will be faced with the potential risk of hostile attacks, such as the nodes are captured or re-disposed by an adversary, or the data of nodes are eavesdropped, interrupted, modified or fabricated and so on. At present, the research on the nodes in based-IOT intelligent household is less, the paper [3] and paper [4] put forward a kind of method of design of wireless network nodes based on nRF2401 or DSP, respectively. The paper [5] focused on the Internet of things smart home wireless sensor network node design， these papers have all been focused on a research on the hardware and the software of nodes, hardly involved the security problem of nodes in the based-IOT intelligent household.

This paper presents a design method of secure nodes in the intelligent household based on the IOT technology, and gives the function model of the nodes, the design of security mechanism and its implementation. From the point of view on node security, to explore how to improve the security of the intelligent household system based on IOT.

2. Nodes Hardware Design

After finished building the nodes of the intelligent household of IOT, all of communications between them are exposed to an open environment, once the illegal nodes have broken through the legal nodes, they could pretend to be the legal nodes, and could imitate the behavior of the legal nodes. The security model of the intelligent household of IOT is included as follows: The nodes should have a safe and stable hardware design to ensure the operation of nodes, the highly effective security mechanisms to ensure nodes security, the intrusion detection to ensure the timely response to attacks.

The main function of nodes in the based-IOT intelligent household is to make the data acquisition and data transmission safe and effective, the nodes module is made up of the processor (CPU), crystals circuit, reset circuit, power supply, antenna and the sensor module. Its structure is shown in **Figure 1**.

The hardware design of nodes needs to ensure the following aspects: low consumption of power, good performance of the radio frequency, miniaturization, low cost, compatibility, etc.

Here we choose the monopole antenna. The length of the $\lambda/4$ of the monopole antenna is:

$$L = 7125 / f \tag{1}$$

In the formula the unit of f is MHz, the unit of L is cm.

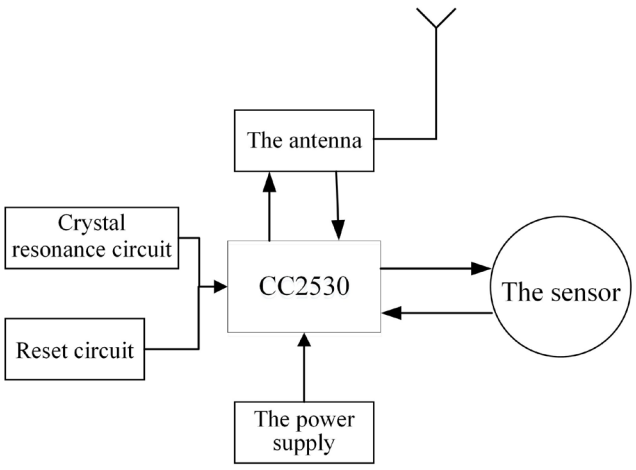

Figure 1. Nodes module.

The single-ended monopole antenna requires a Barron match between the differential output and the antenna. The Barron match can be used in a transmission line form or a discrete components one. The two forms are equivalent to adding a 50 Ω resistor load to the antenna connection. Compared to the discrete components form, the transmission lines one improves the performance of the error vector magnitude (error vector magnitude - EVM entry), the sensitivity and harmonic suppression are also improved, so the transmission line form is adopted in this design [6]. The 3D direction of the monopole antenna is shown in **Figure 2**. At the same time, in the PCB design of the nodes, with the correct segmentation function block, the precise layout line, the reasonable way of decoupling, the reasonable placement of transmission lines and other sensitive devices, it will improve the performance of electromagnetic compatibility of the nodes by this method.

To match the needs of the communication protocols and encryption algorithm in the nodes, here we select CC2530 (256 k) as a network node of the based-IOT intelligent household. CC2530 integrates the single-chip, the ADC and the wireless communication module into one, greatly improved the reliability of combination of the single chip microcomputer and the wireless communication module, moreover, reduced the volume and weight of nodes, the CPU circuit diagram of the nodes is shown in **Figure 3**.

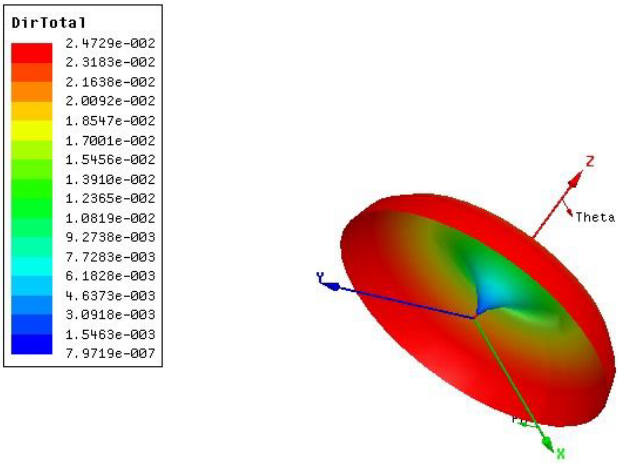

Figure 2. The 3D direction of the monopole antenna.

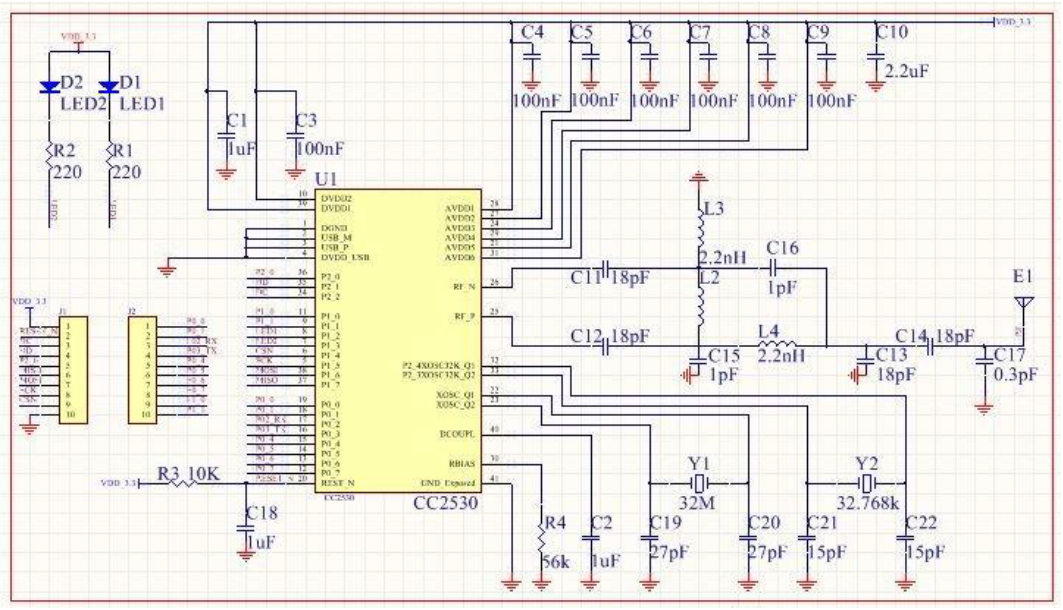

Figure 3. The CPU circuit diagram of the nodes.

3. Security Mechanism of Nodes

On the basis of a good hardware configuration, the security for the nodes of the based-IOT intelligent household needs to establish a security framework to realize confidentiality of data and security of control instructions against the various attacks [7].

The security mechanism of nodes includes four aspects: random key management, access authentication, the encryption and secret communications of control instructions, and intrusion detection and response. Firstly, establishing a random key management system. Secondly, initiating the process of access authentication based on preset-key for nodes. Thirdly, before control commands are transmitted, they will be encrypted by a server or node through the SM4 encryption algorithm, the receiving device will decrypt and recover the control commands on passing the authentication. The process of safe operation of nodes is shown in **Figure 4**.

3.1. Random Key Management

In order to ensure the security of nodes, we use the random key management mechanism to provide nodes with a secret and reliable communication.

The key of nodes in the based-IOT intelligent household mainly includes the authentication key to access the network and the secret communication one between nodes. The former is used to identifying any equipment to access the network, the latter is used for the verification of confidentiality and integrity of communications between nodes. Considering the property of nodes, we build the random key management and periodic updating of key to lower the probability of being attacked.

3.2. Access Authentication

When any nodes request to join the IOT of intelligent household, they need to pass the corresponding access authentication in advance. The soul of access authentication is an authentication of legal identity of node.

The backup node physical addresses Add_n and the secret key k are stored in the center of trust. When any nodes request to join the network, the trust center automatically analyzes the physical address of the secure nodes, and sends a certification of the nodes request. After the nodes receiving the authentication request, they will send the authentication key to the trust center. After passing the authentication of the trust center, the nodes can be allowed to join the IOT of intelligent household. The process of access authentication is shown in **Figure 5**.

3.3. Secret Communication of Nodes

In order to ensure the confidentiality and security of data or control instructions which are sent by the nodes,

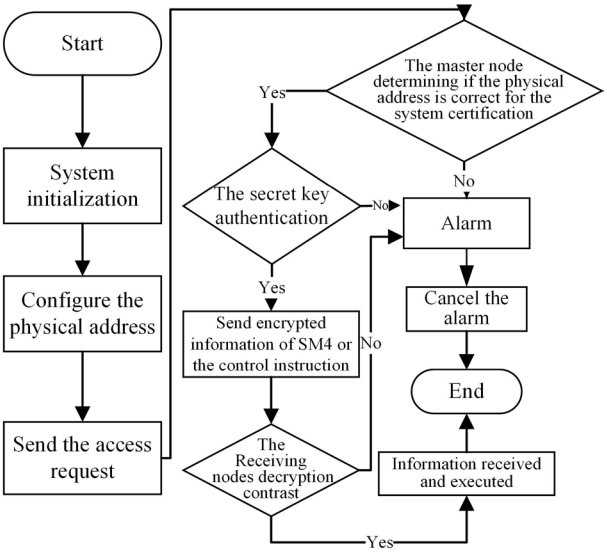

Figure 4. The process of the safe operation of nodes.

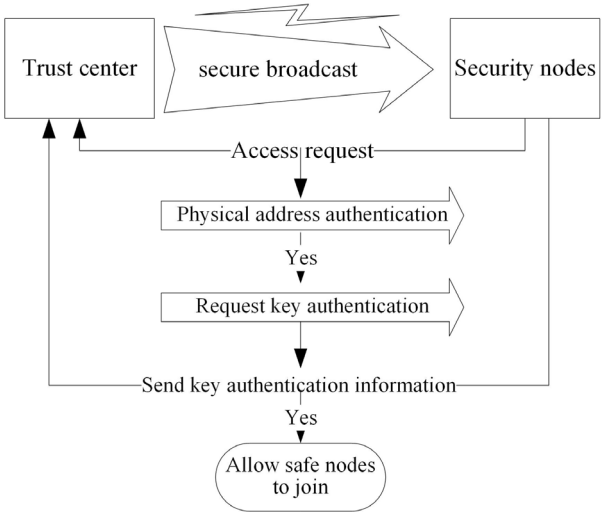

Figure 5. The net key authentication mechanism.

they need to be encrypted before transmitted, this paper adopts the SM4 encryption algorithm [8] [9], the flow chart of encryption algorithm is shown in **Figure 6**.

3.4. Intrusion Detections and Responses

Beyond the random key management and access authentication mechanism above, the nodes must be able to accurately identify any behavior of attack against the IOT of intelligent household, too, to detect and respond any attacks timely and efficiently.

When the nodes detect an illegal action based on the security mechanism above, they will timely alarm and send a warning report to the center of trust, so the based-IOT intelligent household can make timely response to the attack.

4. Tests and Validations

According to the security mechanism of the secure nodes in the intelligent household based on IOT, we set up a point to point testing platform based on the design of hardware, the testing system is composed of a computer, a coordinator of secure nodes and a number of end nodes.

4.1. Access Safety Test

The trust center will store the access keys and the physical addresses of nodes in advance. When any nodes request to join the network, the trust center will require to send the access keys, and to authenticate the physical addresses of the nodes. When the nodes receive the authentication request, they will send their authentication keys to the trust center .The trust center will identify the nodes and then sends the corresponding data to the data window for observation. When the physical address of the nodes and the access keys are correct, the trust center will allow the nodes to join the network.

To test the validity of the mechanism of security, here we imitate an illegal node request to join the network, since the illegal node is unable to provide a correct access authentication key to the trust center, so the trust center will judge the node as an illegal one and refuses it to join the network, meanwhile, it will send an alarm timely. The testing results sample is shown in **Figure 7**, the first column is the key the trust center stored, the second column is the sent key by the nodes to be authenticated. When the key of any node is wrong, the testing window will report the illegal recorder which will be shown in the color of yellow.

4.2. Transmission Security Test

After the passed nodes joining into the network, they will establish the communication each other, such as between node A and node B. Assuming that the node A sends the data of “cquptiotsafetest”, node A firstly en-

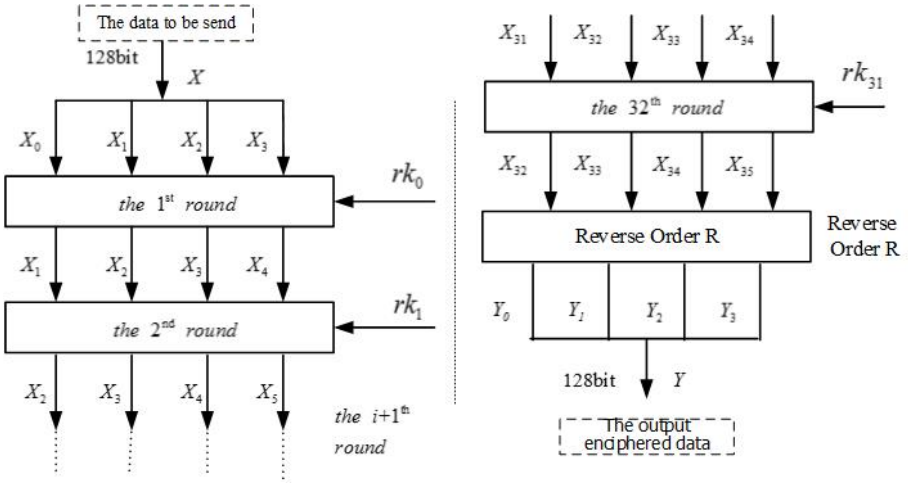

Figure 6. The flow chart of encryption algorithm.

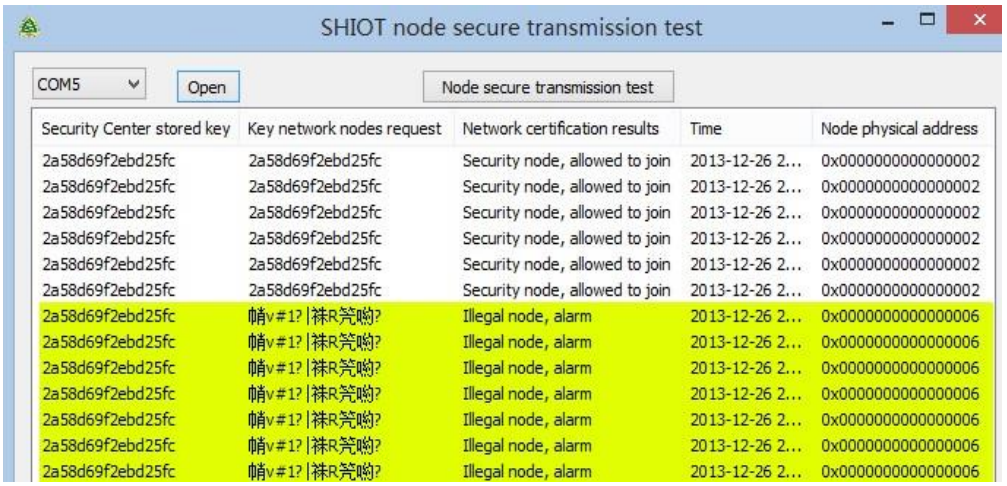

Figure 7. The testing results sample.

crypts the data by using the SM4 encryption algorithm, and then sends the cipher-text to node B. Node B decrypts the cipher-text and obtains a correct data sent by node A, but other illegal nodes will cannot obtain the right data without corresponding key. That is, an error node with the same settings, since the node has already been attacked or tampered or forged, the node is unable to get a right key and pass the authentication, thus it could not access the system and decrypt the cipher-text rightly. In the transmission security test window, we can observe the error nodes which are unable to read the encrypted data, in this way, we can make sure the transmission security of data.

Meanwhile, by the access authentication and the data encryption, intrusion detection and alarm mechanism, etc, we can detect the illegal nodes, the transmission security between nodes test is shown in **Figure 8**.

5. Conclusion

To deal with eavesdropping, denial of service, error instructs, non-authorized access or fabrication and others threats in the based-IOT intelligent household from the adversary nodes, this paper proposed a method of secure nodes based on CC2530, integrated the random key management, the access authentication, secret transmission, and the intrusion detection and alarm mechanism, to realize the security of the communications and control of the nodes in the system. The results of simulation test tentatively show that the proposed method of securing nodes can satisfy the requirements of a secure intelligent household, to be helpful to ensure operations in the based-IOT intelligent household safe and reliable.

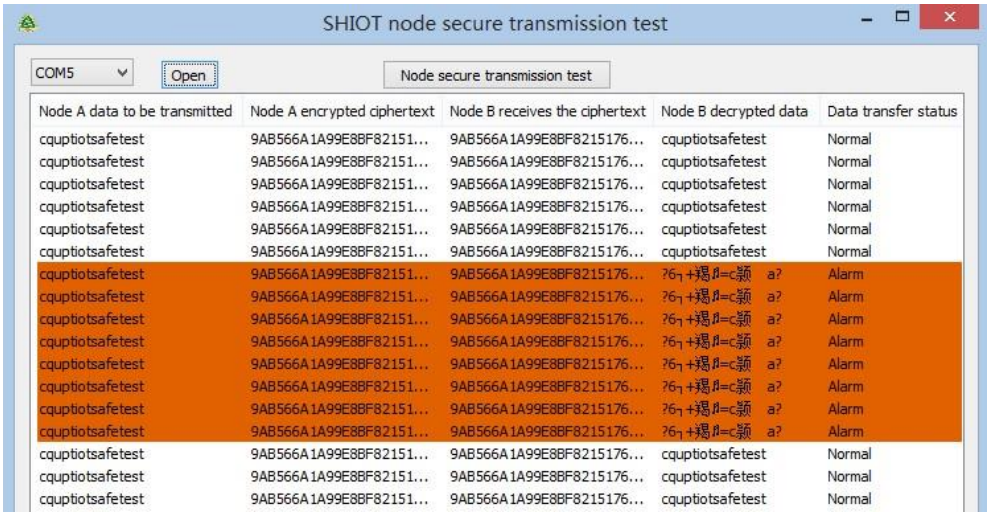

Figure 8. Transmission security test between nodes.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (61170219) and the Natural Science Foundation Project of CQ (CSTC 2013jcyjA40002).

References

[1] Ning, H.S. and Xu, Q.Y. (2010) Global Internet Development and Some Ideas about China IOT Construction. *Journal of electronics*, **11**, 2590-2599.

[2] Zhang, G.Q. and Tang, M., *et al.* (2013) The Spring of Intelligent Household. *Journal of Computer Science*, **S1**, 398-402.

[3] Zheng, J.G. and Wu, C.D., *et al.* (2007) Smart Home Wireless Network Nodes Design Based on nRF2401. *Journal of low voltage apparatus*, **14**, 12-15.

[4] Ni, S.P., Sun, Q.P. and Chen, S.X. (2008) Smart Home Wireless Network Nodes Design Based on DSP Design. *Journal of Engineering Design, and Practices of* 2008, 422-425.

[5] Jiang, Y.Z. and Dong, J., *et al*. (2011) The Internet of Things Smart Home Wireless Sensor Network Nodes Design. *Manufacturing automation*, **1**, 187-189.

[6] Zhao, Y., Feng, R.J. and Wan, J.W. (2007) A High Performance Design and Implementation of the Wireless Sensor Network Nodes. *Electric Measurement and Instrument*, **10**, 53-56.

[7] Yang, J.C., Fang, B.X., Zhai, L.D. and Zhang, F.J. (2012) General Control System for the Internet of Things Security Model Study. *Journal of communication*, **11**, 49-56.

[8] Zhang, B., *et al.* (2012) Practical Security against Linear Cryptanalysis for SMS4-Like Ciphers with SP Round Function. *Science China* (*Information Scienes*), **9**, 2161-2170.

[9] Su, B.Z., Wu, W.L. and Zhang, W.T. (2011) Security of the SMS4 Block Cipher against Differential Cryptanalysis. *Journal of Computer Science & Technology*, **1**, 130-138.