2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing

Construction and Strategies in IoT Security System

Quandeng GOU
School of Computer Science
Neijiang Normal University
Neijiang, China
10602907@qq.com

Lianshan YAN(corresponding author)
Center for Information Photonics & Communications,
School of Information Science & Technology
Southwest Jiaotong University
Chengdu, China

Yihe LIU
School of Computer Science
Neijiang Normal University
Neijiang, China

Yao LI
School of Computer Science
Neijiang Normal University
Neijiang, China

Abstract—The Internet of Things (IoT) is the development production of the computer science and communication technology. As IoT is broadly used in many fields, the security of IoT is becoming especially important and will take great effects on the industry of IoT. Beginning with the concept of IoT, its features and systemic structure, this paper analyzes the security problem of IoT in the stratums of perception, network and application in the system of IoT, puts forward the secure construction of IoT, and offers the corresponding secure strategies based on the existing problems in the framework of IoT. And eventually the theoretical basis will be offered to build up reliable security system of IoT.

Keywords— Network of Things; Security construction; Security problems; Study on Strategies

I. INTRODUCTION

In recent years, with the development of computer science, communication technology and perception recognition technology, the network of things has made a great breakthrough. The IoT can find applications in many fields, from the earliest wireless sensor networks such as the military reconnaissance to the present intelligent transportation, smart grid, smart healthcare, smart agriculture, smart logistics and so on.

The IoT in the future will realize the interconnection between individuals and the expansion between things at any time and in any place, by which a lot of exposed information in public places will be transmitted to the network layer and application layer. However, if the information is lack of effective protection measures, it is easy to be illegally eavesdropped, stolen and interfered. This will certainly pose new threats on the national infrastructure, social and personal information security while preventing the development of the networking industry. Therefore, it is urgent to solve the problem of the information security in the IoT.

Researches on the security issues of the IoT have obtained some progress[1-7]. Literature [1] consider the security construction of IoT from the three aspects (i.e., the node information transmission and information) and elaborates the key technologies in each layer. Literature [2] discusses the security model of IoT based on the classification of security level. Literature [3] analyzes the security needs of the IoT / CPS, proposes a hierarchical security structure, and introduces the security authentication technologies. Literature [4] investigates the four levels of security index system based on three-tier structure of IoT and gets key indicators, such as privacy protection, the WSN anti-attack capability, intelligent node security, which are used to enhance the security of IoT by fuzzy analytic hierarchy process evaluation. and the security attributes of the IoT is mainly reflected in the perception layer. A self-managed security construction is presented in literature [5]. Literatures [6-7] elaborates security scale of the application of IoT, propose a systemic construction of middleware of IoT and apply mature middleware technology as well as safety technology to mask the complexity of security to achieve the security of IoT.

According to the concept, basic features and construction of IoT, this paper not only analyzes the security problems in each layer of IoT system but also provides the appropriate security policy and security strategies, which provides a certain reference value for the practical application of IoT.

II. THE CONCEPT OF IOT AND ITS BASIC CHARACTERISTICS

The IoT is a kind of intelligent system, which uses intelligent objects with perception, communication and computing ability to capture different information in physical world and interconnects the physical objects which can individually addressing. Consequently, overall perception, reliable transmission, and intelligent disposal is realized and the interconnection between people and things as well as among things is constructed[8]. According to the concept of IoT above, it can be found that IoT has three basic characteristics: comprehensive awareness, reliable transmission and intelligent processing. As the first step in IoT system, comprehensive awareness mainly using RFID, sensors and M2M terminal to get the information of the object anywhere and anytime. By the encryption, routing, communication and network security protocols, reliable transmission aims is realized with high accuracy and real-time. Intelligent processing depends on cloud computing, fuzzy recognition and other intelligent computing technology to analyze and hand mass information and pick up meaningful data to meet the different users.

This paper is supported by Sichuan province department of education natural science point item 13ZA0001. School educational reform project JG201224-219.

978-0-7695-5046-6/13 $26.00 © 2013 IEEE
DOI 10.1109/GreenCom-iThings-CPSCom.2013.195

III. THE CONSTRUCTION OF IOT AND ITS SECURITY ISSUES

A. IoT construction

As shown in Figure 1, we can divide it from the network structure into perception layer, network layer and application layer, depending on the three basic characteristics above. The perception layer, the ties between physical world and the virtual world, is the basis of the IoT, whose main task is to achieve reliable sensing. Network layer provides ubiquitous access, information transmission, processing, storage, and the bearer of the core business. The application layer analysis and process the received information to make the right decision and control for intelligent management, applications and services.

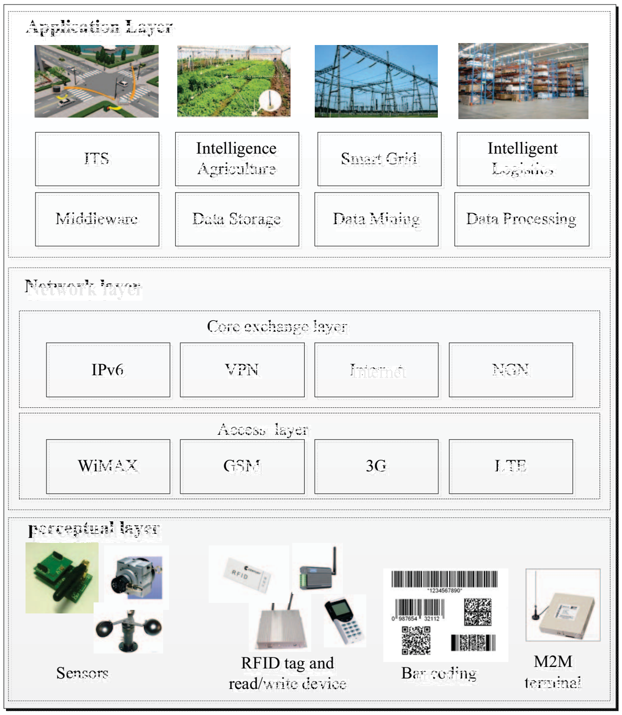

Fig. 1. System Construction of the IoT

B. Security analysis of the perception layer

The perception layer locating in the lowest level of IoT construction, is the source of access to information throughout the IoT. The main security issues includes physical security of sensing devices and the security of information collection. Due to the diversity, simple, energy limited and weak protective capability of sensing node, and mostly deployed in unmanned harsh environment without a special standard, the IoT cannot provide a unified security protection system and is vulnerable to the invasion and attack, which affects the security of the wireless sensor network, M2M terminal and RFID. RFID technology utilizes RF communication to achieve non-contact automatic identification technology. The security problems of RFID including information leakage (the location of the reader and user, the user information and other information), information tracking, replay attacks, cloning attacks, tampering and man-in-the-middle attacks. Wireless sensor network as the perception layer perception data sources, whose information security is very important. The security problems faced in this layer includes nodes physical capture, capture gateway node, sensing information leakage, integrity attacks, energy depletion attacks, congestion attack, unfair attacks, denial of service attacks, forward attack and node replication attacks. For M2M terminal equipment, the risk is mainly due to the deployment before connecting and unattended M2M devices, and thus lead to theft, damage and subscription information attack.

C. Security issues of network layer

Since built on the original basic communication network, IoT faces the risks in existing communication network, including illegal access, data eavesdropping, confidentiality, integrity, destruction, denial of service attacks, man-in-the-middle attacks, virus attack, and the use of factory explores the variety of attacks outside the tools and system vulnerabilities. Moreover, it exists across the network construction network interconnection, inter-network authentication and other security issues, and it may be subject to Dos attacks, man-in-the-middle attack, asynchronous attack, conspiracy attack and so on. At the same time, since the IoT sensing a large number of devices, a variety of formats of the data collected, and the data information has a massive, multi-source and heterogeneous characteristics, Therefore, in the network layer it will also bring other more complex aspects network security issues, such as data transfer needs of a large number of nodes leading to network congestion, resulting in denial of service attacks.

D. Security issues in application layer

The widespread application of IoT is the result of closely integration between computer technology, communication technology and industry professional, which can find applications in many aspects. Besides the business in the traditional communication network abuse such as, replay attacks, application of information security issues such as eavesdropping and tampering, the applications face many extra security issues and become particularly prominent, including cloud computing, middleware, data mining, data storage and backup, management and authentication mechanisms, information disclosure, intellectual property rights, and privacy protection security issues. Currently, how to create a comprehensive cloud computing security framework and cloud security technology has become a research hotspot for cloud computing researchers.

IV. SECURITY CONSTRUCTION OF IOT AND ITS STRATEGY

A. Security construction of IoT

After analyzing the IoT construction layers of the existence of security problems, a safe tiered IoT construction is given, as shown in Figure 2. Physical security is to ensure that the information collection node in the IoT is not destroyed deception and control. Information collection security is to prevent the collection of information from eavesdropping, tampering, forgery and replay attacks, which is mainly related to sensing technology, M2M terminals and RFID security. The security of information transmission is to ensure the process of information transmission data confidentiality, integrity, authenticity and availability of communication network security. Information processes security is data storage, processing and access to the safety and security of cloud computing and middleware. The information application security is to ensure information privacy, the safety of usage, privacy protection, information leak prevention, and application security.

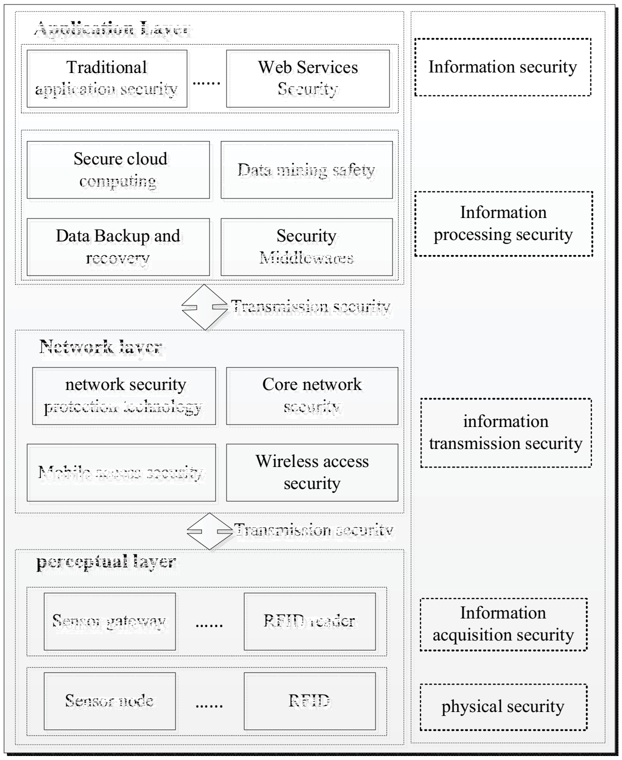

Fig. 2. Security Construction of the IoT

B. Security policies of perception layer

In regarding to sensor nodes in the perception layer of IoT are usually in unattended occasions, vulnerable to vandalism, and even some of the equipment will be stolen, we can redundancy furnishing sensor nodes and replace damaged or stolen sensor nodes in the network key position so that the network can self-heal to protect the physical security of the IoT. In order to solve the security issues of the RFID system, domestic and foreign scholars have made a great effort, put forward many certification programs and achieved certain results [9]. These certification programs are divided into two categories: one is physical security mechanisms, namely to use physical methods to prevent communication between the reader and the electronic tag. Among them, kill command mechanism, electrostatic shielding mechanism, active interference mechanism are utilized to prevent the labeling mechanism, but the defects of these methods are the high cost and low utilization of the label. The second is the authentication security mechanism, namely the use of mature cryptosystem designed to meet the security authentication protocol for RFID systems, such as hash-lock protocol, randomized Hash-lock agreement, hash-chain protocol, interactive authentication protocol, David Digital Book tube RFID protocols, distributed RFID interrogator - response authentication protocol, clap agreement, re-encryption mechanism. For RFID systems, security and cost trade-off are the two main balance factors and thus it is difficult to find a security authentication mechanism suitable for all RFID applications. Therefore, according to the security needs of practical application to divide the corresponding RFID system security level and design appropriate security mechanisms specific security requirements for each level of security.

Combination the perceived characteristics of IoT with the development trend in sensing layer, several suggestions about information collected security are pointed out: (1) From the points of information integrity, confidentiality, authenticity, usability point of departure, divide the perception layer subsystem level of security according to the specific application requirements, to clear each level of security should have the security elements and scope; (2) Strengthen key management system. Due to its limited computing resources, the perception layer network node often chooses a lightweight symmetric and asymmetric key system-based key management protocol; (3) Establish a secure routing mechanism. Secure routing mechanisms is to ensure the correct route discovery, build and maintain target even when network threats and attacks happen; (4) Strengthen the node authentication and access control mechanisms. Authentication and access control mechanisms prevent unauthorized users to access the IoT perception layer nodes and data so that effectively guarantees the perception layer of data security. At present, the sensor network authentication technologies, including lightweight public key algorithm-based authentication technology, based on pre-shared key authentication technology, random key pre-distribution of certified technicians single hash function-based authentication technology; (5) Establish an effective Intrusion Tolerance fault-tolerant mechanism is to ensure the normal operation of the sensing network.

Due to M2M terminal in IoT deployed in the unattended surroundings, it is susceptible to theft, vandalism, and subscription information attacks. M2M devices should have a strong anti-radiation, high temperature resistance, resistance to physical damage, and provide reliable execution environment for M2M. Integrate the machine and card in a single cell, carrying USIM (Universal Subscriber Identity Module) or UICC (Universal Integrated Circuit Card) can not be removed or will be removed and disabled Permanently. If MCIM (M2MCommunications, Identity Module) in the form of software directly bound to the M2M device, you need a special trusted environment M2M device to safely store and execute MCIM, such as remote attestation mechanism in the trusted computing technology[10].

C. Security policies in network layer

For the unauthorized access in the network layer, authentication mechanisms can be used (such as more mature AKA authentication mechanism[11]). When a large number of sensory data or unsafe intrusion data come from the perception layer, filtering and detection mechanism can be used to ensure data security. In order to make the confidentiality, integrity, availability immune in network layer by DDOS attacks, it is necessary to take DDOS attack detection and prevention, including the protection of critical nodes and so on. At the same time, due to the heterogeneity of the network layer connection, information exchange and security vulnerabilities, vulnerable to man-in-the-middle attacks, replay attacks, and combinations thereof attack. End-to-end authentication mechanisms, end-to-end key negotiation mechanism, key management mechanisms and intrusion detection mechanisms can be used to defend against the attacks.

D. Security policies in application layer

When massive data is transmitted to the application layer, in addition to the data intelligent processing, you should consider the security and privacy of data. For data security two aspects should be included: First, data security, access management, security management and modern cryptographic algorithms to encrypt the database. Access management to prevent unauthorized users to use and access the database, security management database administrative privileges are assigned to take security management mechanism, generally divided into centralized control and decentralized control in two ways, database encryption library to encrypt, encryption outside the library, The hardware encryption takes the initiative to protect data; data protection security, data backup, remote disaster recovery and other means to achieve the active protection of the data[12]. Privacy is data owners who do not want the disclosure of sensitive information, including sensitive data, and data representation characteristics, which are divided into common privacy protection technology based on the data distortion technology, based on the data encryption technology, based on the limited release technology, homomorphism encryption technology and privacy agents. In order to prevent unauthorized access to the data, limit their rights, the operation should be based on the level of security or identity, effectively ensuring the security and privacy of data, such as a two-dimensional role-based data access control strategy.

V. Conclusion

Along with the rapid development of the IoT industry, the importance of the security in the IoT is gradually emerging and IoT is one of the most promising network technologies in the new network. In this paper, security issues on the IoT construction layers is analyzed and appropriate coping strategies are given to build a safer IoT construction so that the IoT can reveal healthy and stable development in practical applications. Currently, the researches on IoT safety are still in the primary stage and the safety mechanism is not perfect. Therefore more researchers are need to carry out the in-depth research. In addition to the theory, we should also have a series of accompanying policies, laws and regulations to improve the safety management system.

Acknowledgment

This work is supported by Sichuan province science and technology department the soft science project 2013ZR0089. Sichuan province department of education natural science point item 13ZA0001. Sichuan province academic and technical leader training funded projects 12XSJS002. School educational reform project JG201224-219.

References

[1] LIU Yanbing, HU Wenping, DU Jiang. Network Information Security Architecture Based on Internet of Things [J]. ZTE technology journal, 2011, 17-20(01).

[2] SUN Zhixin, LUO Bingqing, LUO Shengmei, ZHU Hongbo. Security Model of Internet of Things Based on Hierarchy [J].Computer engineering, 2011,1-7(20)

[3] DING Chao, YANG Lijun, WU Meng. Security Architecture and Key Technologies for IoT/CPS[J]. ZTE technology journal,2011, 11-16(01).

[4] Zhang Baoquan, Zou Zongfeng, Liu Mingzheng. Evaluation on Security System of Internet of Things Based on Fuzzy-AHP Method[C].E-Business and E-Government (ICEE), 2011 International Conference, 6-8 May 2011:1-5.

[5] Pierre de Leusse, Panos Periorellis, Theo Dimitrakos, Srijith K.Nair.Self Managed Security Cell, a security model for the Internet of Things and Services[C].2009 First International Conference on Advances in Future Internet,2009:47-52.

[6] SONG Yongguo. Brief analysis of IoT security [J]. Computer Knowledge and Technology, 2011, 2528-2530(11).

[7] YAO yun. The Internet of things security model based on middleware [J]. Computer Knowledge and Technology, 2011,68-69(01).

[8] WU Gongyi, WU Ying. Introduction to the Internet of things engineering [M]. Beijing: china machine press, 2012.

[9] MA Ji-feng,LIANG Hao. Analysis and suggestion on information security of Internet of Things perceptual layer [J]. Modern Electronics Technique, 2012, 76-78(19).

[10] REN Wei, MA Liang-li, YE Min. On M2M Technology and Its Security [J]. Netinfo Security, 2012, 6-9(07).

[11] 3GPP, TS33.102, version9.2.0, 3GSeeurity, 2010, 3.

[12] WU Pufeng, ZHANG Yuqing. An Overview of Database Security [J]. Computer Engineering,2006,85-88(12).