A Survey on the Internet of Things Security

Kai Zhao[1], Lina Ge[1,2]
[1.] School of information science and engineering
Guangxi University for nationalities
Guangxi, China
[2. Corresponding Author] Science Computing and Intelligent Information Processing of Guangxi higher education key laboratory Guangxi Teacher Education University
Nanning Guangxi 530023, China
e-mail: gelina100@gmail.com

***Abstract*—The security issues of the Internet of Things (IoT) are directly related to the wide application of its system. Beginning with introducing the architecture and features of IoT security, this paper expounds several security issues of IoT that exist in the three-layer system structure, and comes up with solutions to the issues above coupled with key technologies involved. Among these safety measures concerned, the ones about perception layer are particularly elaborated, including key management and algorithm, security routing protocol, data fusion technology, as well as authentication and access control, etc.**

Keywords-Internet of Things; Internet of Things Security; perception layer

I. INTRODUCTION

In recent years, with the development of wireless sensor networks, breakthroughs have been made in IoT with wide application. There are great prospects of development and application in IoT, which applied in many aspects of human life, such as environmental monitoring, medical treatment and public health, ITS (Intelligent Transportation System), smart grid and other areas.

The Internet of things [1] refers to various information sensing devices and technologies, such as sensors, RFID (Radio Frequency Identification Devices), GPS (Global Position System), infrared sensor, laser scanner, and gas inductor, etc. It real-time collects object or process which needs to be monitored, linked and interacted. It collects their various demand information, including sound, light, heat, electricity, mechanics, chemistry, biology, location, etc. The purpose of IoT is to connect machine to machine, machine to man, and man to man. It's convenience for identification, management, and control.

With the rapid development of network technology, chip technology plus growing application demands, the Internet of things application scope gradually expands from logistics to smart community, intelligent transportation, precision agriculture and other domains, and its functions also change from traditional tracking management to intelligent control, so as to meet more demands for control. According to EPOSS analysis prediction in "Internet of Things in 2020", IoT development will go through four stages. In 2015-2020 objects will be into semi-intelligent. The comprehensive intellectualized object will appear after 2020. Then IoT will gradually cover all aspects of social life [2].

IoT, as a fusion of heterogeneous networks, not only involves the same security problems with sensor network, mobile communication network and the Internet, but also more particular ones, such as privacy protection problem, heterogeneous network authentication and access control problems, information store and management, etc [3]. The research of IoT security is different from that of Internet security, for it is far more complicated. Therefore, targeted solutions to each aspect of security problems should be made.

II. IOT SECURITY ARCHITECTURE AND FEATURES

Different IoT application fields have differences industry standards and related specifications. Unified IoT structure has not yet formed. However, as to the IoT security standards, many organizations have issued standards such as IEEE, ETSI, etc. Literature [4] gives the development of the IoT security standards. For most of existing IoT solutions is independent small networks, there are relatively few exploits can be attacked. With the sustained development of IoT, the small networks will merge into a large network. By then it would be more difficult to ensure the security. These security problems would be the key factor to decide the development of IoT.

A. IoT Architecture and Security Architecture

The structure of IoT is generally divided into three layers, including perception layer, network layer, and application layer. Some systems take the network support technology (such as network processing, computing technology, middle-ware technology, etc.) as the processing layer. Literature [5] shows IoT system structure divided by the three layers. It makes a summary of the threats and the requirement analysis about IoT security architecture. Literature [6] puts forward a typical model of IoT architecture in the future (U2IoT). It embodies the concept of human central nervous system and social structure. This paper will discuss three layer structures. *"Fig. 1"* gives the architecture of IoT security.

978-1-4799-2548-3/13 $31.00 © 2013 IEEE
DOI 10.1109/CIS.2013.145

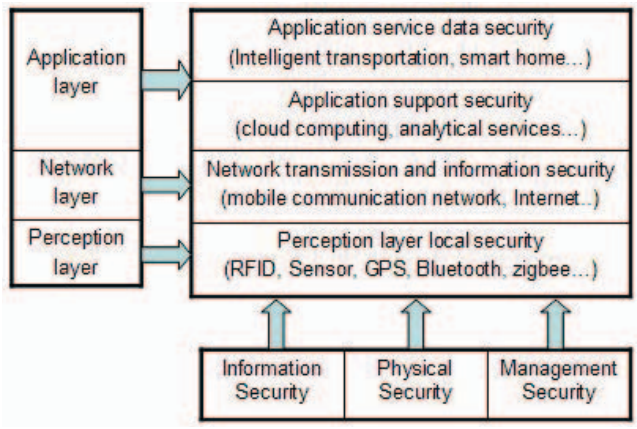

Figure 1. IoT security architecture.

B. IoT Security Features

IoT should have three characteristics: comprehensive perception, reliable transmission, and intelligent processing. Comprehensive perception means by the sensor nodes of perception layer obtain object information anytime and anywhere; reliable transmission means that safely and completely transfer the information of objects through the wireless or wired network to the data center in real time; intelligent processing means that middle-ware analyses and deals with the collected information before submitting to application terminal eventually.

IoT features should reflect the characteristics of IoT security, and reveal the related security problems. In the following security measures, the first three are traditional security features, and others are the new features [7]:

1) The Security Problems of Perception Layer Data Information Collection and Transmission: Sensor nodes have many varieties and high heterogeneity. They have generally simple structure and processor. These make them could not have complex security protection capability.

2) The Traditional Security Issues of Network Layer: Although Internet security architecture has been very mature, there are still many means of attack. For example, a large number of malicious nodes send data at the same time; it will lead to DoS attack. So the specific network should be built for fitting IoT information transmission.

3) The Application Layer Security Problems: For the different application field, there are many complex and varied security issues.

4) The Contradiction between Security and Cost: If each sensor node cost is too low, the large number of low performance nodes will reduce the security of sensor network. On the other hand, high-performance nodes can increase security, but the cost of network maintenance will be improved.

5) Lightweight: The processor performance of sensor nodes is lower, so must be lightweight encryption algorithm and security authentication.

6) Asymmetric: Comparing with network terminal, gateway nodes data processing ability is weak. Nevertheless, how to coordinate these asymmetric networks that need efficient security management measures.

7) Complexity: The types of application determine the number of security issues and complexity. The security problems of each layer should be considered synthetically.

III. The Security Problems of the Internet of Things

As mentioned above, we learn that these problems are complex and difficult. Therefore we need to understand all kinds of security problems of different layer, and potential attacks. Considered the system as a whole, the security problems should be solved at the beginning of the design. Therefore, literature [8] raises the application for the security state assessment about IoT based on grey correlation algorithm, which put several common attacks as the security factor, to realize quantitative evaluation of the entire network about environment and status. It also lists the specific steps that apply this algorithm to do the security state evaluation. In the following paper we will discuss the security problems in each layer.

A. Perception Layer Security Problems

The main equipment in perception layer includes RFID, zigbee, all kinds of sensors. When data are collected, the way of information transmission is basically the wireless network transmission. The signals are exposed in the public place. If it lacks effective protection measures, the signals will be monitored, intercepted, and disturbed easily. The most of sensing devices are deployed in the unmanned monitoring sites. The attackers can easily gain access to the equipment, control or physically damage them. For instance, DPA (Differential Power Analysis) is a very effective attack.

Several common kinds of attack are as follows [9]:

1) Node Capture: Key nodes are controlled easily by the attackers such as gateway node. It may leaks all information, including group communication key, radio key, matching key etc, and then threats the security of the entire network.

2) Fake Node and Malicious Data: The attackers add a node to the system, and input fake code or data. They stop transmitting real data. The sleep of the energy limited node is denied. They consume precious energy of nodes, and potentially control or destroy the entire network.

3) Denial of Service Attack: DoS attack is the most common attack in WSN and Internet. It causes loss of network resources, and makes the service unavailable.

4) Timing Attack: By analyzing the time required for executing encryption algorithm, to obtain key information.

5) Routing Threats: Through cheat, tamper or resend routing information, the attacker can create routing loops, cause or resist network transmission, extend or shorten the source path, form the error messages, increase the end-to-end delay, etc.

6) Replay Attack: Attacker sends a package which has been received by the destination host, in order to obtain the trust of system. It mainly used in the authentication

processing, and destroy the validity of certification.

7) SCA (Side Channel Attack): Attacker attacks encryption devices, through the side channel leakage information in the process of the device operation, such as time consumption, power consumption, or electromagnetic radiation.

8) Mass Node Authentication Problem: The efficiency of mass node authentication needs to be solved in IoT.

In addition, mobile intelligent terminal will be an important part of IoT perception layer. So its security can't be ignored. Now most of the smart phone on the market is given priority to android operating system. However, security verification and high risk of SMS fraud loopholes exist in most android phones, according to characteristics of android system development. Moreover, almost all of the Android software has some function such as scanning phone memory, uploading the user address book, positioning, and collecting users' privacy. Therefore, privacy protection for smart phone users also a problem needs to be solved.

B. Network Layer Security Problems

- Traditional Security Problems. General security problems of communication network will threat to data confidentiality and integrity. Although the existing communication network has a relatively complete security protection measures, there are still some common threats, including illegal access networks, eavesdropping information, confidentiality damage, integrity damage, DoS attack, Man-in-the-middle attack, virus invasion, exploit attacks, etc.
- Compatibility problems. The existing Internet network security architecture is designed based on the perspective of person, and does not necessarily apply to communication between the machines. Using the existing security mechanisms will split the logic relationship between IoT machines. The access networks have multi-access methods. Heterogeneity makes security, interoperability, and coordination of network becoming worse. It easily has security vulnerabilities.
- The Cluster Security Problems. Including network congestion, DoS attack, authentication problem, etc. IoT has a huge number of devices. If it uses the existing mode of authentication authenticate device, a large amount of data traffic will likely to block network. The existing IP technology does not apply to a large number of node identification. The mutual authentication among a lot of equipment causes serious waste of the key resources.
- Privacy Disclosure. With the development of the information retrieval technology and social engineering, hackers can easily collect a large number of the particular user's privacy information.

C. Application Layer Security Problems

In application layer, for different industry or environment, its security issues are also different. At present there are no universal standards for the construction of IoT application layer. But some enterprises carry out M2M (Machine to Machine) mode of IoT, such as intelligent community, intelligent household, medical, etc. Literature [10] puts forward a design scheme of intelligent household security system. Literature [11] gives some solutions that based on 6LoWPAN (IPv6 over Low power WPAN) architecture. They are used for supporting medical sensing system. Although application layer security is more complex and burdensome, it can still be summed up some common security problems:

1) Data Access Permissions, Identity Authentication: Different applications have different users; each application will have a large number of users. So in order to prevent the illegal user intervention, should take effective authentication technology. Spam and malicious information identification and processing should also be considered.

2) Data Protection and Recovery: Communication data involve user privacy. Data protection mechanism and data processing algorithm are not perfect, and it may cause data loss and even catastrophic damage. The mass nodes management is also one reason.

3) The Ability of Dealing with Mass-data: Because of a large number of nodes, a huge amount of data transmission, and complex environment, once the data processing ability and the adaptive ability can't meet the requirements, it will lead to network interruption and data loss.

4) The Application Layer Software Vulnerabilities: When writing software, because programmers write non-standard codes. It causes buffer overflow vulnerabilities exist in the software, etc. Hacker can use these exploits to carry their purposes.

IV. THE INTERNET OF THINGS SECURITY MEASURES

As a Multi-network fusion network, IoT security involves various different layers in IoT. There has been a lot of security technologies applied in these independent networks. Especially, the mobile communication network and the Internet network security research have a long time. For sensor networks in IoT, the diversity of resource and the network heterogeneity make security research much more difficult. This section introducing security measures for each layer will focus on the security technology involved in perception layer.

A. Perception Layer Security Measures

Because RFID and WSN are an important part of IoT perception layer, their security measures will be introduced respectively.

1) RFID Security Measures [12] as follow:

a) Access Control: Mainly in order to prevent the user's privacy leaks, to protect the information in the RFID tags can not be read at will. Including label failure, chip protection, antenna energy analysis, etc.

b) Data Encryption: For the data security of RFID system, it's very necessary to encrypt the RFID signal using the appropriate algorithm. Literature [13] puts forward a kind of nonlinear key algorithm based on the displacement

calculation, and realizes RFID system data encryption. To guarantee under the condition of high speed data transmission, this key algorithm use little computing power, and achieve very high security.

c) The Based on IPSec Security Channel: IPSec protocol suite provides two types of security mechanisms: authentication and encryption. The receiver of IP communication data is able to confirm the sender's real identity through authentication mechanism. Data encryption mechanisms prevent attacker from eavesdropping and tampering data during transmission, and encode data for ensuring data confidentiality.

d) Cryptography Technology Scheme: Cryptography technology not only can realize the user privacy protection, but also can protect the confidentiality, authenticity and integrity of the RFID system. Security communication protocols include based on the hash function, the random numbers mechanism, server data search, the logic algorithm, and re-encryption mechanism.

e) Physical Security Scheme: SCA is a major problem in physical security. The DPA is a common means of SCA. The various strategies which prevent DPA can be divided into two categories in nature: hiding and masking. The hiding eliminates the data dependencies of the energy consumption; the masking makes the intermediate values of the encryption devices by randomized in the process.

2) Wireless Sensor Network Security Measures: As an important part of IoT perception layer, Data is transmitted in free space. The attacker can easily intercept and annalysis data. Therefore, according to different means of attack, need to take the corresponding protective measures.

a) Key Management: The design of security requirements of WSN key management mainly reflects in security of key generation or update algorithm, forward privacy, backward privacy and extensibility, against collusion attacks, source authentication and freshness. There are four main key distribution protocols: simple key distribution protocol, key pre distribution agreement, dynamic key management protocol, and hierarchical key management protocol.

b) Secret Key Algorithms: Key algorithm mainly includes symmetric key algorithm and asymmetric keys algorithm. Asymmetric keys algorithm mainly use RAS (Rivest-Shamir-Adleman) and ECC (Elliptic Curves Cryptography). Symmetric key algorithms mainly use Skipjack and RC5. The processing ability of perceptual nodes is poor. Therefore, symmetric key algorithms are widely used in WSN. Literature [14] puts forward the improved scheme of ECC key management based on the lightweight. It has a wide attention of the key management research in WSN.

c) Security Routing Protocol: The efficient security routing protocol algorithm generally uses the following mechanisms: clustering mechanism, data fusion mechanism, multiple hops routing mechanism, key mechanism, etc. SPINS security framework agreement [15,16] is widely used in security routing technology, including SNEP (Secure Network Encryption Protocol) protocol and μTESLA (Micro Timed Efficient Streaming Loss-tolerant Authentication Protocol) protocol. SNEP protocol is used to implement the confidentiality, integrity, freshness and point-to-point authentication. μTESLA protocol is an efficient flow authentication protocal that based on time. It realizes point to multipoint broadcast authentication.

d) Intrusion Detection Technology: IDS (Intrusion Detection System) can monitor the behavior of network nodes timely, and find the suspicious behavior of nodes.

e) Authentication and Access Control: Authentication techniques mainly include based on the lightweight public key authentication technology, PSK (Pre Shared Key), random key pre-distribution authentication technology, using auxiliary information authentication technology, based on one-way hash functions authentication technology, etc. Access control mainly include based on asymmetric cryptosystem and based on symmetric cryptosystem.

f) Physical Security Design: It mainly includes node design and antenna design. Node design: hardware structure design and security chip selection, chip connection, radio-frequency circuit design, data acquisition unit design; Antenna design should meet good communication distance, high adaptability, stability, etc.

Single measures usually cannot solve the security problem of perception layer; so many measures should be used together.

B. Network Layer Security Measures

In the current structure of IoT, network layer exists based on the Internet or the existing communication network. Some factors endanger information safety on the Internet, and are also damage IoT information service. But the old network communication technology is not completely adapted to IoT. The traditional network routing is simple, and their main goal is not security. Because of IoT node arrangement random, autonomic, unreliability of energy limitation and communication, it leads to that IoT have no infrastructure and dynamic topology. The attacker can easily cause attacks.

For different network architecture, we needs to set up the specific authentication cohesive mechanism, the end-to-end authentication and key agreement mechanism, PKI (Public Key Infrastructure), WPKI for wireless, Security routing, Intrusion detection, etc. Due to the huge amount of data, network availability should be considered. In addition it also should strengthen cross-domain authentication and cross-network authentication in network layer.

Network virtualization technology is widely used. It greatly reduces the complexity of network management, and the possibility of wrong operation.

With the development of next generation network (NGN), and as a transport carrier network in IoT, the construction of IPv6 is followed. Literature [17] gives the development trend of IPv6-based information security products. IPv6 network

security mechanism and application of security products are discussed in detail.

C. Application Layer Security Measures

The Applications of IoT application layer have diversity and uncertainty. It shows up that different application environment have different security needs. There are two main aspects of the measures, technical:

1) Across Heterogeneous Network Authentication and Key Agreement: It includes based on symmetric key crypto-system, based on public key crypto-system (certificate or PKI), and certification transfer technology.

2) The Protection of the Private Information: It includes fingerprint technology, digital watermarking, anonymous authentication, threshold cryptography, etc.

Nontechnical：

1) Increasing the Awareness of Safety: Let users to realize the importance of information security and how to correctly use IoT services. It's in order to reduce the leakage of confidential information.

2) Strengthen Information Security Management: It includes resource management, physical security information management, password management, etc.

V. CONCLUSION

The development of IoT security is an important part of IoT. This paper respectively expounds some problems and solutions from each layer of IoT security structure. But IoT as a big system is integration of several layers, and many security problems come from System Integration so that there are many security problems not belonging to a certain layer, such as privacy protection is involved in each layer.

Therefore, as the application of IoT security technology, instead of doctrinally applying it fixed within a certain range, we must employ various technologies in combination by analyzing particular conditions. IoT security architecture is still in its exploratory stage, so it's facing more severe challenges in security than expected.

ACKNOWLEDGMENT

This work is supported by the Natural Science Foundation of Guangxi Province of China under Grant No.2010GXNSFA013127 & No.2010GXNSFB013052, Science Computing and Intelligent Information Processing of Guangxi higher education key laboratory under Grant No.GXSCIIP201214, Scientific Research Project of Guangxi Province Education Department under Grant No.200911MS72, Science Research Project of Guangxi University for nationalities, Scientific Research Fund of Guangxi University for nationalities, the Fund of Guangxi Key Lab of Trusted Software under Grant No.kx201122, the Program of Science and Technique Foundation of Guangxi Province (Grant No.11107006-30), Scientific Research Project of Guangxi University for nationalities under Grant No.2013MDYB032.

REFERENCES

[1] Hongbo Zhou. Web 4.0: Chinese definition of the Internet of things. Z/OL. China Information World. (37) (2010) (in Chinese)

[2] Huiqiang Wang, Hongwu Lv.: Research on key Technologies and Application for Security of Internet of Things. J. Journal of Daqing Normal University. 32(6): 5 (2012) (in Chinese)

[3] Geng Yang, Jian Xu, etc.: Security Characteristic and Technology in the Internet of Things. J. Journal of Nanjing University of Posts and Telecommunications (Natural Science). 30(4) (2010) (in Chinese)

[4] Mengmeng Sun, Yuan'an Liu, Kaiming Liu. : Security problem analysis and Security mechanism research in IoT. J. Secrecy Science and Technology. (11) (2011) (in Chinese)

[5] Zhuankun Wu. : Initial Study on IOT Security architecture. J. Strategy and decision-making research (2010)

[6] Huansheng Ning, Hong Liu. : Cyber-Physical-Social Based Security Architecture for Future Internet of Things. J. Scientific research, (2):1-7 (2012)

[7] Jianhua Sun, Changxiang Chen. : Initial Study on IoT Security. J. Communications Technology. 45(7) (2012) (in Chinese)

[8] Hongbo Gao. : Study of the application for the security state assessment about the internet of things based on grey correlation algorithm. J. Manufacturing Automation. 34(11) (2012) (in Chinese)

[9] Shancang Li, Kewang Zhang. : Principle and application of wireless sensor network. M. Beijing: China Machine Press (2008)

[10] Xueguang Yang, Fengjiao Li, Xiangyong Mu, etc.: Design of security and defense system for home based on Internet of things. J. computer application. 30(12):300-318 (2010)

[11] Antonio J. Jara, Miguel A. Zamora, Antonio F. G. Skarmeta. : HWSN6 Hospital Wireless Sensor Networks Based on 6LoWPAN Technology: Mobility and Fault Tolerance Management. C. In: International Conference on Computational Science and Engineering, 879-884 (2009)

[12] Lei Li, Jing Chen. : System Security Solutions of RFID System of Internet of Things Sensing Layer. J. Net Security Technologies and Application, (6): 34-36 (2011) (in Chinese)

[13] Xiaoni Wang, Guiying Wei. : Cipher algorithm in data transmission of RFID system on the internet for things. J. Journal of Beijing Information Science and Technology University. 24(4) (2009) (in Chinese)

[14] Geng Yang, Jiangtao Wang, Hongbing Cheng. : An identity-based key distribution scheme for WSNs. J. Chinese Journal of Electronic, 35(1):180-185 (2007) (in Chinese)

[15] Perrig A, Szewczyk R, Wen V, etc. : SPINS:Security Protocols for Sensor Networks. J. Wireless Networks, 8(05):521-534 (2002)

[16] Liu D., Ning P.: Multi-level μTesla: A Broadcast Authentication System for Distributed Sensor Networks. D. North Carolina: North Carolina State University (2003)

[17] Liang Shen, Yan Zhang, Jian Gu. : Development Trend of IPv6-based Information Security Products in Network Layer of IoT. C. In: 27th National Computer Security Academic Communication. (8): 38-40 (2012) (in Chinese)