Study on Security Problems and Key Technologies of The Internet of Things

Xu Xiaohui
School of computer, Wuhan University
School of economics and management, Wuhan University
Wuhan, China
e-mail: sinhui@163.com

***Abstract*—The IOT is a huge and widely distributed the Internet that things connect things.It connects all the articles to the internet through information sensing devices. It is the second information wave after Computer, Internet and mobile communication network. With the rapid development of the Internet of Things, its security problems have become more concentrated. This paper addresses the security issues and key technologies in IOT. It elaborated the basic concepts and the principle of the IOT and combined the relevant characteristics of the IOT as well as the International main research results to analysis the security issues and key technologies of the IOT which in order to plays a positive role in the construction and the development of the IOT through the research.**

Keywords-cloud computing;the internet of things; wireless sensor network; information security

I. INTRODUCTION

The Internet of Things（IoT） is the product and another technology and economic tide of a certain stage of global information development , which will affect a number of major technological innovation and industrial development. Nowadays, more and more governments, enterprises and research institutions put high emphasis on it. Since the construction of the IoT is related to the control and utilization of future network resources, as well as enhancing the domestic capacity for independent innovation and international competitiveness of a range of related industries, thus speeding up R&D of the IoT to promote IoT Industry's rapid development has become a national strategic need[1].The application of the IoT is embedded sensors into a variety of items used in our daily lives, and then integrates it with the existing Internet. In this integrated network, people can realize the remote interaction and management of staff & equipment within the network, which can further increase the level of resource utilization and productivity, thereby improving the relationship between man and nature. However, the current Internet security issues, coupled with is imperfection of sensors and radio frequency identification technology will cause more severe problem to the safety of the IoT. Therefore, study the security issues and key technologies of the IoT will have a significant impact on the safety use and sustainable development of it.

II. OVERVIEW

A. The composition and development of the IoT

IoT is generally divided into three layers: perception layer, network layer and application layer[2]. It is a large scale of information system consisted of the three layers above. It has three features: a comprehensive sense, reliable delivery, and intelligent processing： ① The perception layer, which include smart card, RFID tag and sensor networks, etc, is mainly responsible for the collection work; ② The network layer, consisted by computer, wireless network and wired network and other components, is mainly responsible for the transmission of information work; ③ The application layer completes the analysis of information and controls decision-making, in order to achieve customized intelligent applications and services, and ultimately achieve the connection\identification\control between materials and personals.

This hierarchy determines that the design of security mechanisms of things should based on technical characteristics of each layer and the faced security threats. The core of the IoT safety lies in perceiving security of information collection, transmission, processing and application. Security of things can be described as: awareness of information security, reliable data transfer and secure information handling.

The development of the IoT is divided into three stages: information perception, intelligence material together and intellectual interaction. Information on Internet of things takes the construction of physical objects as a symbol, such as label information, effective document information, building materials joint trading platform, with a static, non-real-time, non-intelligent things together. Sense of things is based on embedded system network, such as smart sensors, smart chip, universal wireless sensor network, embedded systems and other forms of network access, with dynamic, real-time, the wisdom of things together[3]. The interaction stage of the IoT takes the intellectual integration of the whole thing control process as a sign and cloud computing as a starting point. It is the perfection stage of things which makes the interaction among people, goods and network become true and provides a full range material basis to cloud computing.

B. Characteristics of the IoT

Now generally thought of things should have three characteristics: a comprehensive sense, reliable delivery, and intelligent processing. Comprehensive sense means using RFID, sensors, two-dimensional to get object's information anytime and anywhere; Reliable delivery send out object real-time information through the convergence of a variety of telecommunications networks and Internet; Intelligent processing make use of intelligent computing technology

978-0-7695-5004-6/13 $26.00 © 2013 IEEE
DOI 10.1109/ICCIS.2013.114

such as cloud computing, fuzzy recognition to analysis and process the massive data and information so that to implement intelligent control. Although there are different descriptions for IoT, they are in the same logic. Therefore, we will divide it into three logical layers (i.e., perception layer, transport layer and process layer) when we illustrate the security problem of the IoT.

III. THE INFORMATION SECURITY OF THE IOT

A. Terminal security issues of the IoT

As the perception of things has a large number of terminals, and distributed in a large area, information security privacy will be in a great risk if lacking effective monitoring. An attacker can easily access to these devices to cause damage, or even replace the machine's hardware and software through local operation. As the perception terminal of things is responsible for real-time data collection and uploaded them to the network data processing center, data processing center will offer the processed information or decision to the users or interlocks while these perception terminals are the demonstration equipments for that information. More specifically, the major problems related to security concern authentication and data integrity. Authentication is difficult as it usually requires appropriate authentication infrastructures and servers that achieve their goal through the exchange of appropriate messages with other terminal nodes. In the IoT such approaches are not feasible given that passive RFID tags cannot exchange too many messages with the authentication servers. The main problems existed in perception terminals include terminals of sensitive information leakage, tampering, copying, air interface information leakage, terminal virus and other issues.

Since its wireless communication is RFID-based and owns the ability of obtaining information easily, IoT will enable us to live in a "transparent" world if the information security measures failed in place, or there are loopholes in data management. We may face threat from the hackers, virus attacks and etc; objects embedded with RFID tags may also be tracked, located and read which will definitely violate personal privacy of object holder or leak enterprise's secret information. Consequence of these problems are that the legally and orderly use of information are destroyed, human-being life and work collapsed, social system become chaos, and human lives will even be threaten.

B. Sensor network security problem of the IoT

Typically, the sensor terminal's operations are powered by its own battery, and its computing ability, storage capacity, communication ability are restricted by the energy carried by itself which made the design of complex security protocols impossible. Therefore, it hardly owns complex security protection ability[4]. The sensor nodes are not only responsible for data transmission, but also for data acquisition, integration and collaboration. Therefore, the perception network is mainly in the following questions:

① Counterfeit attacks: The intelligent sensor terminals and radio frequency identification tag are relatively exposed to the attackers and the information are transmitted in air in a certain range which make it easy for the implementation of counterfeit attack and highly menace work among sensor nodes.

② Malicious code attacks: Malicious program can easily invade the wireless and sensor network. Its transmissibility, concealment and destructive makes it much more difficult to prevent than TCP / IP network. Malicious code itself such as worm does not require parasitic file, so it will be very difficult to detect and get rid of the malicious code in IoT.

③ Security risks in information transmission and processing: In IoT, information transmission and processing are facing all security issues existing in TCP / IP network. Meanwhile, because of the variety formats of data collected by perception terminate and the large amount of multi-source heterogeneous data come from all kinds of sensor nodes, the network security problem will be more complicated.

From temperature measurement to hydrological monitoring, form navigation to automatic control, sensor network's data transmission and message are without specific standards, so a unified security protection system can be hardly provided.

C. Information transmission security of the IoT

Information transmission safety is mainly related to IoT network layer security while the goal of network layer is to achieve transmission of information and communication, which includes the access layer and the core layer. The security of the network layer is in two main types: The first is from the security risks of the IoT itself; the second comes from the related technologies and protocol vulnerabilities defects of constructing and implementing network function. Because its topological dynamic change leads to trust relationship between nodes are constantly changing, the twig network of things causes a big difficulty to key management. At the same time, as the nodes can freely roam to constantly change relationship with neighboring nodes' communicate ; no statement is in need when nodes join or leave which make it difficult to establish a trust relationship for the nodes to ensure that malicious nodes which mean to destroy the nets does not exist on the path of two nodes. However, the existing mechanisms in routing protocols can not handle this malicious destruction.

IoT's core network should have a relatively complete capacity of security protection, but due to the large number of nodes of the IoT and shows in the way of cluster, then network jam will happen since huge amount of data sent out when transmitting data [5]. Moreover, the existing communication network works in a connection-oriented way, but for wild application, IoT must solve the problems such as address space vacancies and network security standards and so on[6]. According to the current status, the requirements of the IoT on its core network, especially in the credibility, manipuility and controllability, are highly above the capability the IP network can offer. So IoT have to adapt data clustering technology for its core network. In addition, the current security architecture of communication networks are designed from the perspective of human communication, which does not fully apply to communications between

machines, so using the existing Internet security mechanism will split the logical relationship of the IoT machines.

D. Information processing safety of the IoT

Information processing is mainly reflected in the physical security networking applications / middleware layer. Among them, the middleware layer mainly responsible for the interface and function transfer when network layer and IoT service work together, including the of enterprise integration analysis, sharing, intelligent processing, management and so on, embodied by a series of obligations supporting platform, management platform, information processing platform, smart computing platform, middleware platforms, etc. Application layer mainly contains a variety of applications, for example, monitoring services, smart grid, industrial monitoring, green agriculture, intelligent home, environmental monitoring, and public safety and so on.

The security problems of this layer mainly come from all kinds of new services and application business platform. Malicious code and a variety of software vulnerabilities and its mightily own design flaws are one of the major threats to the application system.At the same time as it involves various areas of industry, the technique bottleneck such as safety and reliability for massive data processing and operational control strategies of the IoT are hard to break through. Particularly the environment security problems such as service control and management, business logic, middleware, business system key interface is especially prominent.

E. Businesses security issues of the IoT

IoT devices may connect to the network after deployment meanwhile no one supervises the nodes, so how to deploy remote signing device configuration information and operational information for it becomes difficult. In addition, a large and diverse platform of things necessarily requires a strong and unified security management platform; otherwise the independent platform will be submerged by all kinds of the IoT applications. But if so, how to manage security information such as IoT machine log turns into a new problem, and may split trust relationship between network and service platform, which leads to a new round of security issues.

IV. THE KEY TECHNOLOGIES FOR IOT SECURITY

A. Certification and Access Control

Certification refers to implementation way that the both sides communicated with can confirm the true identity of each other. From the perspective of the IoT system structure, authentication mechanism for perception and network layers is necessary to prevent impersonation attacks and to ensure the validity of the information. Besides, using PKI Public Key Infrastructure to achieve two-way public key certificate-based strong authentication can resolve the physical authentication problem in IoT. Access control technology in the context of the IoT has been given new meaning. It extends from authorization and access control for people to for machines and objects, which effectively blocking the illegal entity access to resources. Access control technology can be correctly implemented just on the basis that certification technology can ensure the entities identification.

Set up rigorous level of authentication and access control for users' who visiting Internet, encrypt passwords, update and authentication, limit users' access directories and files, control network device configuration rights and so on. For example, we can do node to node identity certification before communication; or design a new key agreement scheme, so that the attackers cannot or hardly derive key information from the node information they obtain. Besides, the safety performance of the perception terminal itself can be improved by measures like node design's validity authentication.

B. Data Encryption

Data encryption technology aims to protect the confidentiality and integrity of information transmission and to prevent theft or tampering while transmission. In IoT, two ways of encryption can be taken, that is, node to node (ie, hop by hop encryption) or end to end encryption [7]. The first way is processed in the network layer to realize cipher text conversion on each node, which can be applied to all business, that is, different kind of business can be safely managed in a unified business platform, security mechanisms so that safety mechanism is transparent to business. The end to end encryption execute on the application layer, the sender encrypts only decrypted at the receiving end, you can choose different kind of safety strategies according to business needs, thus business for high security requirements will provide high level of security protection. In IoT, according to different needs, taking different encryption methods will provide security encryption protection in a full range for information.

Data encryption is an important means of protecting data security. The role of encryption is to prevent information from being deciphered when it is intercepted by attackers. Meanwhile, Information Encryption can solve the problem of eavesdropping, but requires a flexible and robust key exchange and management programs which are easy to deploy and fit for the character of scarce sensor nodes resources. In addition, the key management scheme must ensure the entire network security will not be undermined after parts of the nodes are manipulated by attackers. Currently, there is a lot of encryption technology, but how to make encryption algorithm adapt to the fast and energy-saving calculation and to provide more efficient and reliable protection, especially in the case of limited resources, or the relative movement of people and objects to each other in case of faults, to do secure encryption and authentication, IoT calls for a high challenges and requirements to the development of encryption technology.

C. Middleware

If comparing IoT with the human body, the perception layer is like the extremities, transport layer is the internal organs, and the application layer is just the brain, software and middleware is the soul of things and the central nervous system respectively. In IoT, the middleware is located in

embedded devices of integrated server-side ,the perception layer, transport layer of the IoT. In which server-side is called as IoT transaction basis middleware. It is generally constructed upon the traditional middleware (application server, ESB / MQ, etc.), adding devices and modules such as graphical display configuration; Embedded middleware are modules and operating environments which support different communication protocols. The middleware's feature of hiding the details of different technologies is fundamental to exempt the programmer from issues that are not directly pertinent to her/his focus, which is the development of the specific application enabled by the IoT infrastructures. The middleware is gaining more and more importance in the last years due to its major role in simplifying the development of new services and the integration of legacy technologies into new ones. The middleware is characterized by curing many common features, however, in most of the specific application, they need the second-time development to achieve personal business needs, so all the middleware of the IoT required to provide rapid development (RAD) tools. The middleware must include functions related to the management of the trust, privacy and security of all the exchanged data.

D. Cloud Computing

One of the characteristics of the IoT is the intelligent processing, which means using cloud computing, fuzzy recognition and other intelligent computing technology to analysis and process vast amounts of data and information as to implement intelligent control for objects. As a new computing model, cloud computing is a fabulous technical support for IoT. On one hand, the development of the IoT asks for cloud calculation's strong processing and storage capacity. From the volume point of view, a surprising number of sensors will be used to collect vast amounts of data. These data is converged by wireless sensor networks, broadband Internet storage and processing facilities, where cloud computing will do the best. From the qualitative point of view, using cloud computing facilities for data processing, analysis, mining makes physical world management and control be more quickly and accurately and intelligently, so that human beings can manage the physical world more precisely and timely, so as to achieve of the state "Wisdom " that largely enhance resource utilization and social productivity. With its powerful processing power, storage capacity and high performance and low cost, cloud computing will definitely become the background of the IoT. On the other hand, IoT will be the largest user of cloud computing and be the cornerstone for the big business success of cloud computing. However, two key conditions must be considered when fusing cloud computing with IoT :(1) Scale is the basis for combination. It is possible for IoT to combine with cloud computing only when its scale is large enough. Cloud computing is needs in industrial applications, smart grid, earthquake monitor and etc. For the general, local, and home IoT applications, cloud becomes unnecessary.(2) Practical techniques are achieving condition. Appropriate business model and practical services can make IoT and cloud computing better serve human and society.

V. CONCLUSIONS

At present, IoT is still in its early stage and far away from mature. Researches on the security problem of the IoT are still in the conceptual stage which needs further study. Compared with traditional networks, information security, network security, data security and even national security issues accompanied with the development of the IoT are more serious and prominent. IoT cannot be wildly used if it is not safe. Therefore, security issue must be the first consideration in the development of the IoT. Study and solve secure issue that may bring by industry development in advance, strengthen the development of things must be put safety first, ahead of industrial development, strength the legal and technical means, and raise self-protection ability in order to rasp voice and initiative in the new technological revolution and social change.

Although in recent years, international research on this topic is very active, many problems are still controversial. Take the international main research outcomes on IoT security field in recent years as reference, this paper analysis the existing security problems of the IoT, summarizes a few key safety technologies for IoT for the reader to have a brief understanding of this new thing. Overall, I believe that the future research on IoT will focus on the following aspects: IoT security system openness, IoT's individual privacy mode, terminal security, security-related legal system.About how to make IoT into an open, secure, trusted network, we need a long way to go.

REFERENCES

[1] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things,Springer, 2010. ISBN: 978-1-4419-1673-0.

[2] Yan L, Zhang Y, Yang L T. The Internet of Things:From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications, 2008.

[3] Atzori, Luigi,Iera, Antonio,Morabito,"The Internet of Things: A survey",Computer Networks, v54, n15, October 2010,pp.2787-2805.

[4] LEUSSE D,PER IORELLIS P,DIM ITRAKOS P. "Self-Managed Security Cell, a Security Model for the Internet of Things and Services Advances in Future Internet".2009 First International Conference on Digital Object Identifier,2009,pp. 47-52.

[5] OLESHCHUK V, Internet of things and privacy preserving technologies, Wireless Communication, Vehicular Technology, Information Theory and Aerospace& Electronics System s Technology,Aalborg: [s. n.],2009.

[6] MEDAGLIA CM,SERBANATI A," An Overview of Privacy and Security Issues in the Internet of Things", The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications, New York: Springer New York,2010,pp.389-394.

[7] SAVRY O,VACHERAND F, Security and Privacy Protection of Contac less Devices [M].the Internet of Things:20th Tyrrhenian Workshop on Digital Communications, New York: Springer New York,2010: 409-418.