Internet of Things Security Analysis

GAN Gang
Network Engineering College
Chengdu University of Information Technology
Chengdu 610225, P.R. China
test_me@cuit.edu.cn

LU Zeyong
Network Engineering College
Chengdu University of Information Technology
Chengdu 610225, P.R. China
lzyluzeyong@163.com

JIANG Jun
School of Computer Science
Chengdu University of Information Technology
Chengdu 610225, P.R. China

***Abstract*—Internet of Things is an up-and-coming information and technology industry, and in such an environment of the concept and the content and the extension of Internet of Things are not very distinctive, the project of Internet of Things which is a piece of small area with small-scale and self-system obtain gratifying achievement and bright future, it can promote the development of Internet of Things in some extent. But there are some serious hidden danger and potential crisis problems. The paper focuses on the application of Internet of Things in the nation and even in the global in the future, analysing the existed security risks of the Internet of Things 's network points, transmission, finally we propose some suggestive solutions due to these problems.**

Keywords- Internet of Things；Sensor；RFID

I. INTRODUCTION

Internet of Things ,Bill Gates mentioned in "The Road Ahead" in 1995[1].Then in 2005,ITU published Internet Report forecast it's establishion will bring 1 billion the order of the information equipment, the order of 3.0 billion intelligent electronic devices, 500 billion off the microprocessor, the sensor needs more than trillion. Truly, Internet of Things is a huge boost engine in the future information industry, is the third bid wave of the information industry in computer network.

What is the Internet of Things? Through RFID, infrared sensors, global writing system, laser scanners and other information sensing equipment, connecting any object with Internet for information exchange and communication services. Ultimately, to achieve intelligent devices located, tracked, monitored and manage the functions of a network, to make the physical infrastructure and IT infrastructure integration.

Internet of Things is "Material objects connected to material objects in the Internet." There has two meanings can be explained: in the first place, the Internet is not only the core and foundation, but also based on and extension of the Internet. Another place, Client's extension and expansion make links between every things and any objects, generate information communication.

II. STRUCTURE

"Information Superhighway" is more professional name of Internet of Things, which can be divided into three key levels[2].The first layer is the most basic perceptual level (also known as recognition layer),collecting information and identifing the physical world .The middle layer is the network layer (also known as wireless sensor networks), which responsible for the information transmission, initial processing of information, classification and polymerization. The topmost and terminal level is the application layer, which provide the services for all industries.

Among the three levels, network layer can be said a "Central Nervous System" that provide universal services in the Internet of Things, because it plays the role of combining with application layer upward and produces the link of perceptual layer downward. There are several basic network which are wired network, wireless network, mobile or a private network provide and support the underlying connection. Business application of Internet of Things is set up in these networks composed a new network[3].The structure shown in Figure 1:

Figure 1. Internet of things structure figure

III. SECURITY REQUIREMENTS

Network layer, has several properties. Requirements security of sensor storage, processing and transmitting information and prevents unauthorized accessing even illegal operation, called confidentiality. Asked to each node which participate in information processing is authentic reliable, call

978-1-4244-7255-0/11/$26.00 ©2011 IEEE

authenticity. Requests the transmission of information has not been tampered or destroyed without authorization, with along integrity. Request every gateway working and provide best services, as availability. The sending and receiving data must be latest and updated, not the attacker modifing, definition as Data Fresh. In addition, with the characteristics of low-cost, disposable, unattended, sensors are easy damaged, broken up and physical access even controlled. Therefore, wireless sensor network require scalability and false tolerance. Or in such circumstances like some nodes working abnormal, adding new nodes and adjust nodes, like maintaining a large number error-prone and easily controlled sensors' network that requires infinite self-organization and automatically network. Then, the properties of network that have relationship shown in Figure 2:

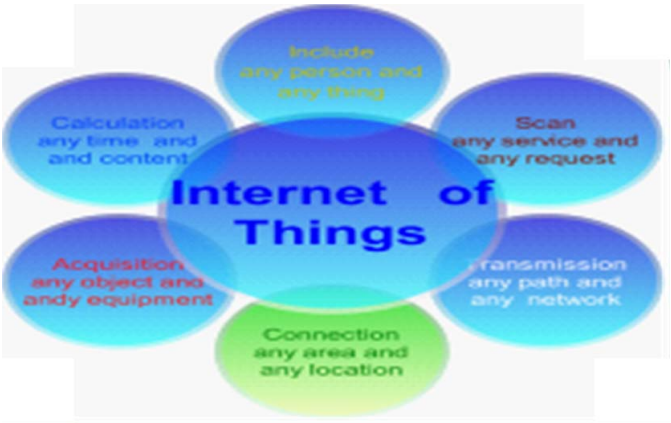

Figure 2. Internet of things structure figure

IV. PAY ATTENTION TO THE SAFETY

The relationship between Internet of Things and Internet is inseparable and complementary. However, not the same in the form of network organization and in network functionality and in performance requirements of the two networks. Internet--based on the priority management typical characteristic make it not very require safe, reliable, controllable and manageable. But, Internet of Things heavily dependent on some aspects includeing real-time, safe and reliable, resource assurance.

Along with Internet of Things brings new technologies rising, Information security escape from periods which are traditional virus infections, hackers and misusing of resources, forward a complex and diverse, comprehensive interactive period. In addition, Internet of Things mainly consists of sensor network and M2M parts which can be seen as sensor module and network layer constitute a large network together. One point should be taken seriously, massive levels of network terminals and signal source exposed in a public place, if the network transmission control system or software have problems, the consequences is very serious.

Currently, Internet 's development encounter two big system bottlenecks problems , one is the IPv4 address is not enough, the other is the network itself security[4].Through IPv6 resolve address deficiencies, however, there isn't a good solution for the current network security. In a word, network manageable, controlled and service quality issues are not deal well, to achieve accurate, efficient, real-time network signal transmission is castles in the air, and will affect the further development.

V. SECURITY ISSUES

Wireless sensor network's characteristics present new challenges in information security area. Along with one-time, unattended, wireless communications, low-cost and resource-constrained ,sensors easily appear to abnormalities, physical attacks by attackers, Trojan attacks, virus damage, keys decryption, DOS, eavesdropping and traffic analysis are really threats. The trouble is a challenge that design of key storage, distribution, encryption and decryption mechanism caused by wireless sensor network 's large and resource constraints[5].

In the traditional system, network layer security and application layer security is independent, just as communication between the leaderships and communication between the secretaries is different. Internet of Things is on the basis of the existing mobile network platform integrate sensor networks and Internet that make large amount of special problem of it. This situation can be said combine with leadership and secretary. Therefore, most of the mobile network communication system can still be applied to Internet of Things and provide security as authentication encryption and mechanisms. However, according to the characteristics of the network layer, we need to adjust the system and add functions. For example :1)sensor network gateway nodes out of control ,2)network 's DOS attacks to sensor network nodes, 3) interference, tampering and destruction to the network signal, 4) the problems including identified large number of sensor nodes, identification, certification and control.

A. Encryption gateway node

Obtain the ciphertext without the key cannot decipher the plaintext. Similarly, when the gateway node encrypted, capture a node is not equal to control the node, such a sensor node is hard to be controlled because attacks need master key of the node.

In this way, integrate the key that is sensor network internal communication nodes and the key that is the remote information processing shared platform as a important key node. Who want get the key is very difficult in this case, which get a gateway node has not shared key with sensor network , he can not control gateway node and get all information through it .Then he can not tamper with the sending information ,only prevent some or all information are sent , but it would be easily detected by the remote information platform. In this case, when an administrator found an abnormal sensor network , he will take some appropriate measures to reduce even avoid a great loss that caused by abnormal network sending false information.

B. Enhance the capacity against DOS attack

Sensor network must connect with external network eventually including the Internet, so they can not escape

attacks form other network . Currently, exclude the main attack illegal access, the other may be DOS attack. Since sensor network nodes resources which are computing and communications capabilities are limited, so the capacity against DOS attacks is weak. In the Internet environment, a DOS attack access that is not found can make the sensor network serious damage even paralysis. Therefore, sensor network nodes should have the ability to fight against DOS attacks, considered a direct access to the specific node inside net, such as remote control infrared system startup and shutdown, ordinary nodes inside have less resources than gateway nodes ,so the capacity against DOS include both the gateway nodes and the ordinary nodes two types.

Sensor networks connect with other network brings the problems which is not only it against external attacks, but also is how to authentication external device. So in the certification process, we must pay much attention to limited resources of sensor networks, then authentication mechanism we designed that the computational cost and communication cost must be as small as possible. In addition to the external Internet, the connected with different sensor networks' number may be a huge , how to distinguish between each network even nodes inside, how to identify them effectively, all of those are the premise to establish security mechanisms

C. The encryption mechanism

The traditional network layer use by-hop encryption mechanism that information in the transmission process need to keep decryption and encryption in each node make every node transmission in " clear text ", even encryption at the begin of sending. And similarly, the traditional application layer encrypted end to end, which can be explained the " clear text " in the sender and the receiver, each node is ciphertext in the transmission time. As Internet of Things ' network layer and application layer connect closely, making us face using by - hop encryption or end to end encryption in the transmission.

For by-hop encryption, it provides the protection to links which asked necessary. Due to by-hop encryption in the network layer so that we can apply to all business, which make different applications safety implement and management on the one network platform. In this way, security system is transparent to the business applications.

By - Hop encryption ensure low latency, high efficiency, low cost and scalability characters. But, because the by-hop encryption requires decryption in the transmission nodes, so every node is likely to interpret the clear text message. In a word: by-hop encryption demands high trustworthiness on the transmission nodes.

As for the end to end encryption, it can choose a different type business security policy, in order to provide high security protection for applications required high level security. However, end to end encryption can not protect the destination address. Because each node through which a message should be as the destination address to determine how to transmit messages. This make end to end encryption not hide the message's source and destination, which is easy attacked by malicious access cause by analysis of the communication services. In addition to the perspective of national policy, end to end encryption can not meet the national demand for the lawful interception policy.

From these analysis, the security requirements of some business is not very high , under the environment that network can provide by - hop encryption protection, end to end encryption is not very important in service layer requirement. But, to the high-security business, end to end encryption is still the first choice. Thus, due to the different requirements to the different security levels in business, we can see end to end security in service layer as another option.

As Internet of Things have started to accelerate develop, the security requirements of it is increasingly urgent, we need to figure out the special security requirements, then consider how to provide end to end security protection. How to use existing mechanisms resolve these security features? The concept of the machine cluster is introduced by Internet of Things ' development, because of it, also need to outsider how to use machine group solving authentication problems.

Now days, Internet of Things is developing in the primary stage even just a hot concept, not to talk about its implementation structure, etc. Thus, the safety mechanism of it is a blank in the industry, it is a long way for it's research for and establish up.

D. Business authentication

The traditional certification distinguish different levels. For example, authentication of the network layer is responsible for the network identification, the same is to the application layer. Most of cases in Internet of Things, a machine has itself special function, so the business applications and network communication tied together closely. As the network layer authentication is essential and so the application layer authentication no longer is necessary. Who design it also can provide services and applications degree by himself opinions.

Give some examples.When the application of Internet of Things provided by the carrier ,you can take advantage of the network layer authentication results not the application. layer 's.When the services provided by a third agent and can not obtain key parameters ,it can initiate independent certification without considering the network layer .And when the business is sensitive such as financial services, generally service provider do not trust the security of network and choose higher level security protection, it is the time need to be done in the business layer certification. When business is normal application, like the temperature collection services etc, the provider think it is sufficient, so not need the certification of application layer.

E. Own unique problems

According to Internet of Things ' characteristics , it faces not only the traditional mobile communication network security issues but also some special security issues different from existing 's. This is because it is constituted by a large number of machines, lack of effective monitoring and

management, which is large number equipment and cluster cause. These special problems mainly in the following areas.

Internet of Things' machine--identify local node safety issues. Since some applications of it can accomplish and replace complex, dangerous and mechanical work, so the machine equipment are deployed in unattended outdoor scene, the attacker can easily access to these facilities and replace the parts of equipment and chip implanted Trojan horses, the consequences is unimaginable. These things will be designed and implemented well in the future, must set up early warning systems and even automatic isolation.

The security issues of data transmission and information in sensor network. Sensor nodes usually have single function as temperature measurement and carry less energy, making their have not complex monitoring and lacking of defense capacity. But ,the identify of the sensor network varieties form temperature measurement to hydrological monitoring, form road navigation to precise positioning, which have no specific criteria for the data transmission and the message signals. So we can not provide a standardized security system, structure and the law.

The security issues of how to transfer data and signal in the core network. Core network with relatively complete protection and defense system, but, due to Internet of Things has large number of nodes and working in cluster , which maybe cause DOS service attacks by network congestion in transmission. Therefore, we must consider the load balancing algorithm for branch large amounts of data. In addition, the existing communication network security architecture is for human not fit for physics objects communication, separating the existing security mechanisms in machine - object and object - object logic relationship. Therefore ,we must change the views in the implementation and the design process of it, to form a material-center ,human-traction scheme.

The issues of Internet of Things application security. As it may be first networked devices then connected to network, it is impossible to guard for the nodes in time, which is a big time-consuming problem how to sign remote configuration and business information. There will be a strong and unified security management platform for a large and diverse network.Otherwise, independent platform will be overwhelmed in all kinds of network applications. How to manage logs and informations network become a new problem, how not to separate network and service platform trust relationship. These will be lead to a new security problems.

VI. Conclusion

"The Future of The World, must be intelligent virtual world , must be cloud computing and Internet of Things world. " With the technologies of it developing and deepen promoting. The three networks which are Internet of Things ,The Internet and 3G mobile wireless network will continue approach together. The more develop Internet of Things, the more intelligent of it .While more areas of social has been widely application, the social will become information society in material to material and object to human[6].

Meanwhile, we can not ignore the security implications, because signal loss will directly affect the whole security of Internet of Things .Due to viruses, Trojan horses, hackers , malicious software are powerful and popular, which may restrict our travel and prevent us communication with others by invading our mobile phones. When virus running in our computers, we can stop and cut network to prevent the spread of virus. But what and how to do in this case, that virus spread in the network that the whole world become only one , are we prepared to deal with it? In fact, building Internet of Things is not only technical problems, but also involve in planning, infrastructure, management, security and other aspects problems. All this will require appropriate policies supporting and regulations even strengthen building of technologies.

References

[1] Zhao Hai-Xia. Internet of Things ' key technology Analysis and Discussion[J].Western Technology China,2010.4
赵海霞.物联网关键技术分析与探讨[J]. 中国西部科技，2010.4

[2] Tan Xue-Qing, Fu Rui-Ping, Gao Qian. Identification is the Foundation of Internet of Things[J]. Automatic Identification Technology of China, 2009
潭雪清 付瑞平 高倩. 物联网识别是基础[J]. 中国自动识别技术，2009

[3] Zhou Shuang-Yang. Find the High Place in Internet of Things[j]. Communication World A, 2009
周双阳. 寻找物联网制高点[J]. 通信世界 A，2009

[4] Bo Hong-Mei.Analysis Internet of Things' technology[j].Technology Information Communication. 2010.
薄红梅. 浅谈物联网技术[J]. 科技资迅，2010

[5] Zhao Zhang-Jie,Liu Hai-Feng. Wireless Sensor Network Security[J], Computer Security , 2010
赵章界 刘海峰. 无线传感网络中的安全问题[J]. 计算机安全，2010

[6] Huang Hai-Kun, Deng Jia-Jia. Internet of Things Gateway Nodes, Technology and application[J].Telecommunication Science,2010
黄海昆 邓佳佳. 物联网网关键技术与应用[J]. 电信科学，2010