# The Internet of things era information security challenges and coping strategies

Su Cai, Li Xueqiang, Li Jing, Wang Hong

Qingdao Huanghai University, Qingdao Shandong 266427

**Keywords**：Information security, The Internet of things (IoT), challenges, Coping strategies

**Abstract**：Internet of Things (IoT) security research mainly concentrated on the Internet security system, Internet of individual privacy protection mode, the Internet of things security related legislation, etc. This paper analyzed the challenges of IoT based on the present situation, and then some corresponding countermeasures are provided in the final analysis. It is an early warning that we should give enough attention to the development of IoT.

## Introduction

Cloud computing and Internet of things (IoT) have increasingly become to a global trend of development, and it will change the industrial pattern and social life. Everyone uses the Internet, and everything is on Internet. Because wireless transmission is needed in many occasions, the public information has turned to be very easy to steal. This phenomenon will directly affect the safety of Internet of things. And it leads to new challenges to the information security. The influences of unitary virus infection, the website hacking and the resources abusing as traditional security issues are not forbidding any more, but we step into a more complex new period which is full of comprehensive interaction.

## Applications of the Internet of things (IoT)

Network security of IoT research is an emerging field, any security technology are accompanied by a specific application. Therefore, the safety study of Internet of things will always run through in people's lives. The application of the Internet of things is to embed the sensor in various items in our daily life, and then combined the "Internet of things" with the existing Internet, so that people could do remote interaction and management personnel and equipment, which improves the relationship between human and nature under the continuous improvement and utilization of resources and productivity.

Intelligent transportation involves in many aspects. As the RFID highway toll charge system, it uses the automatic vehicle identification technology to realize wireless communication between vehicle and toll station. It transfers the automatic vehicle identification into the charging data, and then completes the whole toll charge process without car stopping. The train control network supervises controls and adjusts the state of the train speed and braking mode according to the actual situation and the objective conditions of the train running on the railway, which can achieve automatic continuous monitoring to avoid vicious accident of manmade operation error and to ensure the safety of high-speed train.

The Intelligent logistics use read-write electronic tag to realize efficient. Establishing auto perception and intelligent control system for logistics based on the IoT technology and attaching

unified E-tags on all kinds of products are efficient ways to accomplish quick send and receive operations and the whole process dynamic monitoring from production line to warehouse by automatic identification and orientation classification. The use of radio frequency identification and satellite positioning technology in the logistics system can complete the operation and management for those important materials. So far, WAL-MART and other large retail institutions have realized the application of intelligent logistics.

The use of networking can also realize intelligent Home which can take part in family security and monitoring. It can do counter-terrorism monitoring for of the airport and other key area form a perimeter intrusion sensor network system by using optical fiber. In China, surveillance cameras have been widely used in a number of major roads, hot spots, subway and residential areas. Embedded RFID students card can detect students' entering and leaving time at school, and parents can be noticed and track their children promptly to make sure their safety.

**Internet security challenges**

The Internet of things in the perception layer during data collection, the mode of information transmission is the basic wireless network transmission, signal of the exposure in public places, if the lack of effective protection measures, it is easy to be illegal eavesdropping, theft, and interference; application in the Internet, a large amount of sensors used to mark items of equipment, by remoting control or computer to complete some complex, dangerous or high precision operation, in this case, these items in IOT devices are mostly deployed in unattended place to complete the task, then the attacker will easily access to these devices, which can damage to these devices or the bearing the sensor, even by decoding the sensor communication protocol, the illegal manipulation of them. To perceive information through one or more connections with the outside network sensor node, called joint network All communication, and sensor network internal nodes need to go through the gateway node contact with the outside world. So the security problems faced by the perception layer mainly manifested in the following aspects: the existing Internet security protection have relatively complete, but because of the number of nodes in the Internet are huge, this will easily lead to a large amount of data sent at the same time the sensor network node, received from a network of denial of service attacks; gateway node sensor network by adversary controlled - Safety lost; common node sensor network is captured, for intruders attack on the Internet of things provides the possibility; identification, ultra large number of sensor nodes access to IOT identification, authentication and control problems.

The perception layer of IoT usually gains by the wireless network transmission. Compared to the TCP/ IP network, there are infinitely many malware entrances in the wireless network environment and sensor network environment. These exposures in the public are easily invaded if you don't have proper protection, such as the worm of malicious code that, once it gets a successful invasion, it will be hard to prevent from its dissemination, concealment and destruction. In such an environment, it will be difficult to remove and detect malicious code like this, which will directly affect the networking system security. Internet of things has highly dependence on the Internet, any harm of information security factors exists in the Internet may lead to a harm to IoT to a certain extent. With the development of the Internet, virus attack, hacker intrusion and illegal access will cause damages to the Internet users.

Secure communication between nodes is the main contents of IoT security. Most of the time, IoT is operating under non-supervising. So it is necessary to reduce the destruction of nodes to ensure the physical security of the Internet of things. We can take the following measures: identity authentication is the key point to prevent counterfeit attack. Because measures sensor nodes can be easily physical manipulated, therefore, it is necessary to authenticate the nodes. Through

authentication, both sides of communication can confirm the authenticity of the other party, and strengthen security authentication between node and node, node and network, to ensure the legitimacy of the node. In addition, you can also exclude the illegitimate nodes in the network, the way is that treat the adjacent nodes as the third party certification. Before communication, we can authenticate nodes by symmetric or asymmetric cryptography code scheme, at the same time, we should promote node security when we do the speed limit of sending data packet and limited number of data packet retransmission. Access control is based on identity authentication which is aimed on authorizing to different users after authentication according to different user identity. When we carry out the access control, we should be strict in the user password encryption to increase the difficulty level of decryption for intruder. The administrators should divide users into different access authority, set user permissions by its own restrictions when they access to the data to ensure data security and privacy. It can enhance the security of the entire network with equipment configuration permissions,.

In order to strengthen the protection of networking security transmission, security level of network transmission protocol should be improved, and also improve networking sensor node hardware. Effective measures include: restriction networking node packet transmission speed and the same data packet transmission times. It can make up for lack of network security protocol. The data packet reduces the speed in the transmission link, the node resources will be full or almost full, so the intruders do not have enough resources to operate, the transmission node attacks on the Internet of things will be limited. On the other hand, limit the number of times of same data packet content transmission and destroy the source data immediately after packet transmission, even if node the invaders invaded, they also cannot get the source data. It can ensure the security of the data in a certain extent.

The traditional IP network usually has two kinds of encryption forms: point-to-point encryption and end-to-end encryption. However, the current technical architecture recognized that both encryptions are hard to implementation in a certain degree. This is because, in the node layer, if you want to run an encryption/decryption procedure, you not only need the overhead high-speed CPU and memory, but also need a lot of resources and consumption of nodes. Therefore, the problem now we need to solve is to find a balance between safety and efficiency in order to meet the demand of IoT data encryption. A good key management standard is: it must be easy to deploy and suit for sensor nodes. How to do security encryption and authentication under limited resources is further demands on the encryption technology of IoT data. There are two kinds of key management in the Internet of things: private key encryption algorithm and public key encryption algorithm. We can be combined with the use of two kinds of encryption algorithm. For large capacity data encryption we use private key encryption algorithm, and private key encryption algorithm can be encrypted by public key encryption algorithm. It can effectively improve the efficiency of encryption, and simplify the key management.

In order to ensure the development of the Internet of things, to create more economic and social benefits, Internet of things (IoT) should strengthen its efforts on research and technology development. Sensor is the core technology of the Internet of things (IoT), it can transfer the physical quantity and chemical quantity into electrical signals, and solve the problem effectively. By now China mainly uses the foreign sensor technology and facilities, the ability to master the core technology is still not enough, self-research and development ability is relatively weak. Governments at all levels should strengthen the implementation of preferential policies, and vigorously support enterprises which develop a new type of implementation of networking equipment, encourage small and medium-sized enterprises to carry out technical research and

development, and breed competitive high tech enterprises in IoT security technology with international market competitiveness. Also, Capital, incentive system, personnel support and other supporting systems should be fully guaranteed.

At present, we should establish policies and norms that could adapt to the development of IoT as soon as possible, including the safety of participants, information security and privacy protection, in order to protect security mechanism of industry.

Then establish management department for IoT is necessary. It should be unified, and its rights and functions are strengthened, so the IoT security work can realize the authoritative information security management system, and form a security mechanism from the corresponding management system.

Strengthen people's awareness of self-protection. On the basis of sound legal and regulatory laws, people's awareness of self-protection should be increase in order to promote the development of the Internet of things (IoT) to develop in depth.

## Concluding remarks

Internet of things (IoT) is a new real-time interaction system between virtual and the real world. Its characteristics are ubiquitous data aware, wireless information transmission and intelligent information processing. The popularization and application of Internet of things (IoT) technology significantly improves the economic and social operation efficiency, it also presents a serious challenge on the issue of information security and privacy protection of country, enterprise and citizens. Therefore, the relevant departments have to absorb the experience and lessons from the past to avoid the disadvantages, research on the issues that may occur during the development process, then formulate related rules through legal, administrative, economic and other means, in order to solve all kinds of social conflicts and new social relations caused by the development of Internet of things (IoT). Regulate IoT legal application will lead to an open, secure and reliable network with effective legal and policy support in China.

## Acknowledgement

Project funds :Field project”Shandong wisdom - Internet of network information security research on legal support and guarantee system”2014

## Reference

[1] Shao Xiwen. Study on the safety of Internet of things based on RFID (J). Computer engineering and application, 2012,48 (S1).

[2] Liu Yanbing, Hu Wenping, Du Jiang. Network information security system based on Internet of things (J). ZTE technology, 2014 (17).

[3] Wang Zhiwen, Deng Shaoling,. Characteristics of information security of Internet of things and preventive measures (J). Science and technology information, 2014 (12).

[4] Teng Ping. Networking in information security and prevention measures of J. Network technology and application of safety, 2013 (3).

[5] Ye Meilan, Wang Linlin. Social risk and policy supervision in the perspective of Internet of things (J). Journal of Nanjing University of Posts and Telecommunications (Social Science Edition), 2013 (6).