The Perceptual Environment Security Mechanism Research for Internet of Things

MA Shideng[1, a], Huang Hai[2,b]

[1]Neusoft Institute, Guangdong, foshan 528225, China

[a]mashideng@126.com

Keywords: Internet of Things, Perceptual Environment Security, RFID, WSN

Abstract. The Internet of things has become the computer and the Internet after the wave of new information technologies. The goal of the Internet of things is a comprehensive perception, on the basis of Internet technology and platform, to build a person connected to the object, content and the content of the platform. The deepening of the research in recent years, along with the Internet of things, and the Internet of things applications of expansion, it to the further development of information society brings new change, at the same time, Internet information security problem also gradually aroused the concern of the industry is larger.

Introduction

With the maturity of the RFID technology and the rapid development of mobile intelligent terminal, with more attention paid to the Internet, will become another revolution after the Internet. However, compared with the traditional Internet applications, using RFID equipment and intelligent terminal as the supporting technology of Internet of things applications, is more complex more serious security problems. Such as trust mechanism, privacy protection, reliable routing and malicious behavior detection, has become a pledge to build security network to solve the key problems, the thorough analysis and research for the improvement of the Internet of things the security of the infrastructure and the whole Internet security system is of great significance [1-2]. In this paper, on the basis of summarizing the existing work, some key techniques for Internet security problems were studied. Iot's perception of the environment is relatively complex, perceptual node of affiliation, service demand differences and credibility, based on the secure routing credible data at the same time, maintain a highly efficient and reliable routing protocol.

Perceptual layer technology of Internet of Things

Perception as the core of Iot, its three basic characteristics are: comprehensive perception, reliable transmission and intelligent processing. Respectively by the three parts of the Internet of things perception layer, network layer and application layer.

The Internet of things technology core is the perception layer, it similar to the role of the human body skin and facial features, used to perceive objects and gathering information. Perception layer consists of sensor network and sensors of two parts, mainly including radio frequency identification technology, WSN sensor technology, global positioning system (GPS), laser scanning, infrared sensing, video technology, barcode scanning, etc. In recent years, radio frequency identification technology and WSN sensor technology has achieved rapid development.

Radio frequency identification technology. RFID is a non-contact automatic identification technology, emerged in the 90 s. As a rapid, real-time, and accurate information about the acquisition and processing of high and new technology, the technology is recognized as one of the top ten key technology in this century [3]. RFID generally includes three components of electronic labels, readers and antennas. It adopts radio frequency method, can realize the two-way data communication, identify the target object and obtain relevant data. The RFID system composition is shown in figure 1.

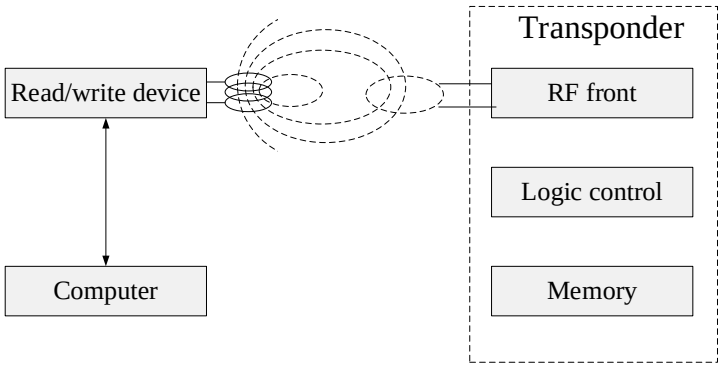

Figure.1 System schematic diagram of the RFID

WSN sensor technology. A sensing technology is a multi-discipline blend of modern science and technology, it mainly studies on the natural objects access to information, and to recognize and deal with it. Sensor is the core of the sensing technology, it can be something in the Internet of things and objects between information interaction between people. Wireless sensor network (WSN) is composed of a large number of micro sensor nodes, the nodes are deployed in the monitoring environment, form a self-organizing wireless communication network. WSN perception, data collecting and processing the entire network of perception object information, and send the information to the observer [4]. WSN flaw is that it can only get a scalar information perception object, as a result, wireless multimedia sensor network arises at the historic moment, it is on the basis of WSN increased access to images, voice, and video data, such as the function of information. WSN architecture is shown in figure 2.

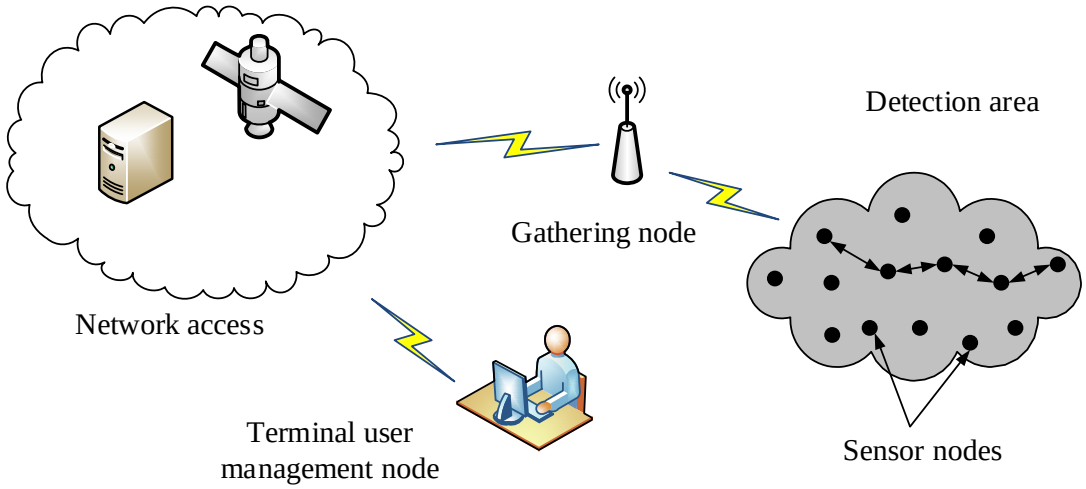

Figure 2.Architecture of wireless sensor network system

The perceptual environment security analysis for Internet of Things

As mentioned earlier, aware of layer two key technology of the physical world information is RFID and WSN sensing technology. Therefore, this paper discusses the Internet of things awareness of information security, RFID and WSN sensing technology should be considered two aspects of security [5].

RFID security. In iot perception layer system structure, each RFID is a single network node, they were through the gateway access to the network layer. As a result, each node is decided by the information security of RFID RFID for the whole system framework of information security. RFID security issues embodied in the following aspects:

(1)Information leakage. When RFID tag users without knowing, attackers illegal copy or steal label information, lead to goods information was leaked.

(2)Label tracking. The attacker using fixed on the RFID tag information, tracking and positioning, lead to privacy was leaked.

(3) Replay attack. Attacker by some special means, hacking into items of information transmitted to legitimate reader, again to attack system.

(4) Copy attack. RFID tag information of the attacker duplicate legitimate users, the legal user's identity, and that, in turn, to attack system.

(5) Forgery attack. The attacker to forgery of RFID tag information, forge the information content and legal user's identity, cost information and user identity authenticity.

(6) Information to tamper with. The attacker to deliberate tampering or message, lose information integrity, then after to tamper with the information sent to the original receiver.

WSN sensing technology security. The characteristics of WSN nodes is limited resources, storage capacity, communication ability and handling ability is limited, and topological structure of complex, etc. Its technical security issues focused on the following two cases:

(1) Physical damage: a WSN node distribution in natural space, the attacker can use external means, and is easily implemented on a node of damage, physical modification on them and use them to interfere with the normal network node operation. Internet caused by common node capture the key leak, security threat, or due to complete control of the entire network security threats.

(2) Attacks: the attacker by various ways of network attack, form a security threat. Such as depletion attack, congestion attack, not fair attack, denial of service attack multiple identities, node, copy attack, attack, etc.

The perceptual environment security mechanism for Internet of Things

Aimed at the safety problems of IoT perception layer, the following technical scheme is put forward.

1) The RFID security technology

Label protection. The RFID electronic tag play an important role, and the electronic tag information is easy to steal, copy, forged and tampered with. Therefore, the electronic label protection measures is particularly critical. The most effective measures to control the use of the label is conditions, set up under the condition of a certain tag. In the specific application, when the goods completed, in order to prevent leakage of label information, RFID tags can "kill" goods, or make it into "hibernation" state, make tags cannot work normally.

Encryption mechanism. The password techniques, in accordance with the contract, is both parties to a communication rules to transform information of a confidential technology. Based on the cryptography, using cryptographic algorithms and security authentication mechanism, to implement the RFID system to protect information security, is a hotspot of research on the current Internet of RFID encryption mechanism. Many security authentication protocol was put forward, including Hahs-Lock protocol, Hash chain, the Hash-base IDvarition agreement, David digital library RFID protocols, interaction and LCAP protocol and distributed authentication protocol RFID ask - response authentication protocol, etc.

2) WSN security technology

For WSN security protection, should strengthen the key management control, to set up the security of WSN routing, adding nodes authentication, access control mechanism, intrusion detection mechanism of management style.

Key management. WSN key management mode can be divided into a symmetric key encryption and asymmetric key encryption. Symmetric key encryption communication is typical of the two sides use the same key, use this key to encrypt the sender and the receiver also use this key to decryption. This key encryption key length is not long, computing, communication and storage cost is relatively small, more suitable for WSN, it is the mainstream of WSN key management way. Rather than the symmetric key encryption is refers to the nodes use different encryption and decryption key.

Security routing. Iot of special structure makes it right by the higher safety requirements. , therefore, should according to different application requirements, the Internet use appropriate

security routing protocols, to ensure that the data safely from one node to another node. At the same time, should be as less as possible consumption node resources, and the efficient operation of the node. Iot security routing technology has to use SPINS security framework, which includes SNEP protocol and mu TESLA two parts.

The node authentication. Node authentication can prevent unauthorized users access to the Internet of things perception layer nodes and data, the effective protection of perception layer information security. At present, the main nodes in sensor network authentication techniques are: authentication method based on lightweight public key algorithm, based on the pre Shared key authentication method, random key pre distribution method of authentication and authentication method based on one-way hash function.

Access control. Access to the network information resources must be based on an orderly access control premise, for different visitors, should stipulate their operation privileges, such as whether is readable, writable, whether to allow modification, etc.

Intrusion detection. Intrusion detection is a kind of active protection system from attack of network security technology, it through some key node in the network to monitor and collect information, and the analysis, find out problems, blocking and track in a timely manner, the nodes of the network behavior monitoring, timely find suspicious behavior. Distribution of nodes in the Internet of things is very extensive, and the security is relatively weak, so appropriate USES distributed intrusion detection system.

Conclusion

The current environment, the Internet of things got rapid development, however, the security problems to a great extent, restricts the further development of the Internet of things. As the Internet of things technology core, perception layer information security is the key to effectively promote the development of China's Internet of things could continue to. In this paper, the Internet of things, the cognitive layer technology in information security on perception layer is analyzed, in view of the sensing layer are two key technology of RFID and WSN sensing technology some safety technical measures are put forward.

References

[1] Guinard D, Ion I, Mayer S: /Mobile and Ubiquitous Systems: Computing, Networking, and Services. Springer Berlin Heidelberg, 2012: 326-337.

[2] Li X, Lu R, Liang X: Communications Magazine, IEEE, 2011, 49(11): 68-75.

[3] Barnaghi P, Wang W, Henson C: International Journal on Semantic Web and Information Systems (IJSWIS), 2012, 8(1): 1-21.

[4] Zhou L, Chao H C: Network, IEEE, 2011, 25(3): 35-40.

[5] Bandyopadhyay D, Sen J: Wireless Personal Communications, 2011, 58(1): 49-69.