International Journal of Mobile Computing and Multimedia Communications
Volume 10 • Issue 1 • January-March 2019

Security Model of Internet of Things Based on Binary Wavelet and Sparse Neural Network

Zhihui Wang, School of Information Science and Engineering, Hebei North University, Zhangjiakou, China
Jingjing Yang, School of Information Science and Engineering, Hebei North University, Zhangjiakou, China
Benzhen Guo, School of Information Science and Engineering, Hebei North University, Zhangjiakou, China
Xiaochun Cheng, Middlesex University, London, UK

ABSTRACT

At present, the internet of things has no standard system architecture. According to the requirements of universal sensing, reliable transmission, intelligent processing and the realization of human, human and the material, real-time communication between objects and things, the internet needs the open, hierarchical, extensible network architecture as the framework. The sensation equipment safe examination platform supports the platform through the open style scene examination to measure the equipment and provides the movement simulated environment, including each kind of movement and network environment and safety management center, turning on application gateway supports. It examines the knowledge library. Under this inspiration, this article proposes the novel security model based on the sparse neural network and wavelet analysis. The experiment indicates that the proposed model performs better compared with the other state-of-the-art algorithms.

KEYWORDS

Binary Wavelet, Internet of Things, Security Model, Sparse Neural Network

1. INTRODUCTION

The Internet of Things is usually composed of a large number of unattended sensor nodes. The traditional intrusion detection system is difficult to adapt to the power source of the sensor node in the Internet of Things that limited computing ability and limited storage space. Therefore, it is lightweight and Reconstruction is a feasible way to meet the requirements of intrusion detection applications in the context of Internet of the Things. Government, enterprises, scientific research institutions more and more attention to the Internet security issues, for the perception of equipment security Some technical means, including the high-intensity encryption CPU card, RFID tags for the certification, key management mechanism and from the production process using the anti-power consumption/electromagnetic radiation analysis, the fault injection attack technology and so on. Can you see whether these safety precautions are effective on the one hand? Does it meet the relevant standards? It needs to be further clear (Lee, et al., 2013; Perera, et al., 2014; Whitmore, et al., 2015).

DOI: 10.4018/IJMCMC.2019010101

Internet security issues involving the network equipment based security, network security, Web security, and based on many aspects, such as Web application security, especially in the Internet of things in this article the Internet part, its content mainly includes security coding, safety and key management and exchange data frames. We firstly review them as the follows.

- Key management and exchange: In the Internet implements the confidentiality and the complete measure key lies in the key the establishment and the management process, because in the thing networking node computation ability, power source ability and so on are limited that causes traditional the key management way not to be suitable under the thing networking the Internet.
- Security code: Since any one of the label identification or identification code can be remotely scanned arbitrarily, and the label automatically, without distinguishing the response to the reader and the information stored in the reader to the reader, so the security of the code must be taken seriously (Al-Fuqaha, Guizani, Mohammadi, Aledhari,& Ayyash, 2015).
- Security: data frames in the Internet information dissemination environment, an attacker could eavesdrop on content of the basic data frame, access to relevant information prepare the way for further attacks (Tao, Cheng, Xu, Zhang, & Li, 2014).

The Figure 1 shows the particularity of the composition of the Internet of things, both has the solid facility equipment, and has the intelligence transmission which the network moves. Moreover after its equipment usually deploys the general networking first, therefore, the thing networking node mostly is at nobody guarding the condition, besides has the mobile communication network tradition network security question, but also has some with to have the migration network security different special security problem as follows.

- Radio frequency identification technology used in the Internet of the Things system, RFID tags are embedded in each piece of material, the user to use, transport materials, the end device or RFID cardholder without the knowledge of the circumstances, the information is read, or in a certain In the middle of the channel, the information is intercepted halfway, and the user or owner of material is uncontrollably scanned positioned and tracked without any notice.
- The attacker usually first to find the system vulnerability, and then access to system privileges, and then the implementation of the destruction, tampering or theft of system data. Because the terminal sensor nodes in the Internet of things are deployed in a large number of clusters and the number is huge, it is even more terrible for the attacker to spread malicious code or to implement buffer overflow attack through the intrusion node. Compared to the TCP/IP network, its dissemination, concealment and destruction will be more serious, but also more difficult to prevent (Lin, et al., 2014;Bi, Wang, & Bao, 2015).
- Due to the openness of the deployment of the Internet of things application, including the perception of a node or terminal equipment configuration in the unmanned surveillance, usually hard to protection, there is perception nodes are easy to be the attacker physical damage, such as using replace safe hidden trouble, and may even end of the "Trojan horse" chip implanted devices, so as to steal the sensing information.

Considering the mentioned challenges, this paper proposes novel security model of Internet of Things based on binary wavelet and sparse neural network. As a result of thing networking constitution particularity, both has the solid facility equipment, and has the intelligence transmission which the primary network moves. Moreover after its equipment usually deploys the networking first, therefore, the thing networking node mostly is at nobody guarding the condition, besides has mobile communication network tradition network security question, but that also has some with to have the migration network security different special security problem.