A NEW SYSTEM FOR WIRELESS SENSOR NETWORK INFORMATION SECURITY BASED ON HIERARCHICAL INFORMATION INTRUSION DETECTION

[1]D.Ramya, [2]B.Ramesh Chandra Goud, [3]A.Rakesh, [4]Bhatuka Madhavi
[1,2,3]Assistant Professor, [4]UG Student, [1,2,3,4]Department of Computer Science Engineering, Brilliant Grammar School Educational Society Group of Institutions Integrated Campus, Hyderabad, India

ABSTRACT
Attacks on computer networks are becoming more severe and more frequent. The majority of currently available security solutions focus on thwarting one or more threats. The use of computer networks has become a necessity in people's daily lives. In addition to successfully increasing productivity and quality of life, it may also reduce travel time between individuals. E-banking, e-commerce, and other wireless sensor network services are discreetly influencing people's lives in today's society. People should actively use firewall, encryption, network access control, and network virus prevention technologies for effective protection in order to successfully prevent these information security issues. In an effort to increase security and stability, this study examines the mechanisms for protecting information security and evaluates the security issues associated with the use of wireless sensor networks through effective measures.
Keywords: Computer network, Network information security, Wireless sensor networks.

I.INTRODUCTION

With the recent advancements in sensor, computer, wireless communication, and distributed information processing technologies, wireless sensor networks are a novel technology [1]. Especially in the military sector, the application environment of wireless sensor networks is typically complicated. The foundation of its use is how to make wireless sensor networks secure [2]. A wireless sensor network is a sizable self-organizing network in which a lot of inexpensive, resource-constrained sensor nodes collaborate to complete a particular goal [3].

With the rapid development and maturity of microelectronic technology, computer technology and wireless communication technology, wireless sensor network has been gradually applied to military, environmental monitoring and other fields, and has gradually entered the practical stage [4]. This kind of micro sensor network with computing and communication capabilities is a multi hop self-organizing network formed by a large number of cheap micro sensor nodes through wireless communication, which can complete the data collection, transmission and fusion of various monitoring objects in the deployment area in a cooperative way [5].
Today's network has become an indispensable part of people's life, and people's demand and dependence on information network system are also increasing. At the same time, the threat of network technology development to networksecurity is becoming more and more serious.China's computer network started late, but with the development of China's economy, network information technology has madegreater breakthroughs, and has developed to a relatively mature stage, which is used by citizens in all aspects of social life [6].
In order to solve these security problems, people have developed and applied various security mechanisms, security policies and network security tools. This paper summarizes the basic theory, analyzes the current computer network information security problems, and finally puts forward a computer network information securityprotection strategy based on wireless sensor networks (WSN) [7].

ANALYSIS OF NETWORK INFORMATION MANAGEMENT SECURITY

Computer virus is a common executable program code, which has certaindissemination and destructiveness, and destroys the security of Internet information structure. After the execution of computer virus, it will reduce the efficiency of the system, at the same time it will damage or delete files, resulting in data loss, damage to the system hardware and various unpredictable consequences [8].

Analysis of the Characteristics of Sensor Networks:

The network topology of most sensor networks is unpredictable before deployment, and the whole network topology and the role of sensor nodes in the network often change after deployment. Network connection is a process in which all sensor nodes meet and gather, and it is also a process in which sites meet in the pre-data transmission stage. In this process, there may also be artificial damage to networkconnection.

According to the above analysis of wireless sensor characteristics, wireless sensor networks are vulnerable to many threats and attacks, such as physical manipulation of sensor nodes, eavesdropping of sensor information, denial of service attacks, disclosure of private information and so on. Although the computer network has been popularized on a large scale, there are still some computer users who lack the awareness of network security and do not pay attention to the installation and update of anti-virus software and firewall system, thus making personal information leaked and network security not guaranteed.

In the actual attack process, advanced equipment can be used to frequently send data packets to the wireless sensor network, which makes the communication within the wireless sensor network blocked, or advanced equipment can be used to disguise as a base station to monitor the wireless sensor network [9].

Potential Threats in Wireless Sensor Networks:

Network security means that the software and hardware of the network system and the data in the system are protected and will not be damaged, changed or leaked due to accidental or malicious factors. Most of the common hacker problems in the network occur in this process, they will consciously screen and intercept the network data, and after illegally invading the computer,personal privacy information will also be stolen.

Compared with traditional wired network, wireless communication is easier to be monitored [10]. By injecting bit stream, the previous data packets can be simply replayed. However, the establishment of wireless sensor networks usually has no technical staff, and after the equipment is placed in a certain place, it completely depends on the equipment itself to run [11].

This mode of operation makes the acquisition of network nodes very simple. After the attacker finds the corresponding nodes, he can replace them with other sensors or directly rewrite the memory, so that he can monitor the whole wireless sensor network. Once the computer network has security problems [12], it is very likely to cause incalculable consequences andlosses.

COUNTERMEASURES OF INFORMATION SECURITY PREVENTION IN WIRELESS SENSOR NETWORKS

Network Access Control Technology: In the normal operation of computer network security system, it is necessary to set certain access rights and use information encryption technology. To a certain extent, access control is a kind of information technology used by all systems including computers, which is mainly to avoid illegal intrusion into the subject, and then to protect users. From the perspective of computer network security managers, we shouldstrengthen the management of local areanetwork, correct our working attitude, improve the network security management process, build a good computer network operating environment, and realize theeffective promotion of professional andtechnical level.

Network access control technology is often used in network security prevention and protection. It is generally divided into network access control, network authority control, network server security control and attribute

security control, which can effectively ensure that network resources will not be illegally used or accessed.

In actual operation, encryption technology can turn important data into garbled code for transmission, and the receiver can restore the data through corresponding decryption technology, thus effectively preventing the information from being eavesdropped or interfered during transmission. Future sensor networks generally have hundreds of sensor nodes, so it is difficult to monitor and protect each node. Therefore, each node is a potential attack point, which can be physically and logically attacked by attackers.

Compared with network firewall, data encryption technology has higher security and is more suitable for open network environment.

At the same time, data encryption technology can also protect the dynamic information of computer system in real time, which can not only intercept the invasion and attack of other programs in the first time, but also effectively prevent passive attacks and improve the security of computer system. In order to improve the application effect of computer network security measures, it is very critical and necessary to optimize and improve the software application and usage rights.

Network Virus Prevention Technology:

In real life, the setting and application of network firewall can help us resist the access and attack of foreign users, improve the security of computer network, avoid potential security risks, and effectively restrain the network management behavior. Network virus prevention technology is mainly to set up some comprehensive virus prevention software, and ensure that the software can be automatically upgraded, and automatically pop up relevant instructions in operation, so as to prevent virus invasion.

For enterprise computer systems, after LAN connection, it is necessary not only to resist and prevent Trojan viruses and system vulnerabilities, but also to strengthen the prevention of "hacker" attacks. Computer network security management has a long way to go. In order to implement the decisions of the decision-making level, it is necessary to have a management level to manage the daily work and an implementation and maintenance level to be responsible for the implementation of safety plans and decisions. The hierarchical information security organization is shown in Figure 1.

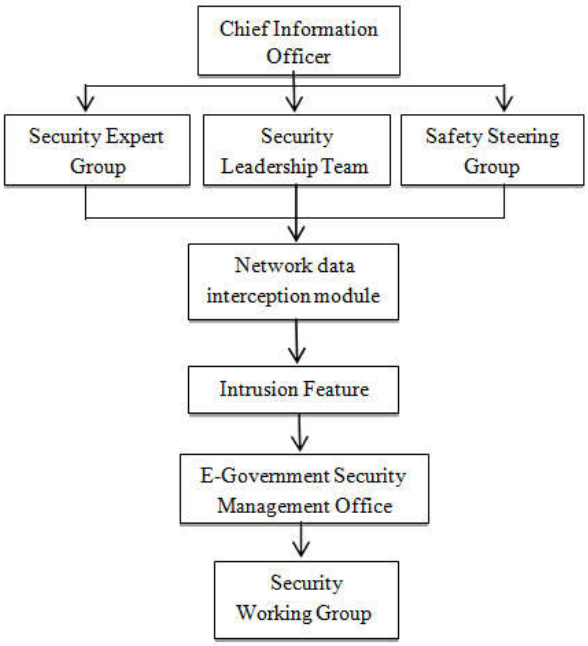

Fig.1: HIERARCHY OF INFORMATION SECURITY ORGANIZATION FOR INTRUSION DETECTION.

One of the common methods used by hackers is to crack the administrator account and password, so it is

necessary to reconfigure the administrator account. The economic and reliable operation state. Antivirus software should be installed in the computer network system, so as to timely check and kill the virus that has been invaded. If you can't check and kill the virus, you should update the virus library to check and kill. If still unable to check and kill, the virus should be uploaded to the anti-virus website for help.

RESULTS

An ad-hoc network topology with 30 nodes is built, and the Ad-hoc On-Demand Distance Vector (AODV) routing protocol isemployed. We use and modify an existing wireless sensor network simulator in MATLAB for the simulation tests. Four datatraffic follows are set, and the simulationtime is 100s. Four kinds of attacks are deployed: 1) Black Hole; 2) Jelly Fish that delays all forwarded data packets; 3) routingspoofing that repeatedly send deceptiveroute error messages to make the source node invalidate the current using route; 4) unauthorized access to networks. In this simulation, the unauthorized node always imposes Jelly Fish attack simultaneously. The attackers, i.e., the Black Hole, unauthorized (with Jelly Fish), and routing spoofing nodes are gradually added to the first step is to establish a complicated password for the ADM initiator account. Then we rename the administrator account name, and build an administrator account without administrator rights to createillusion for intruders. As shown in Figure 2, the structure of the intrusion detection system is explained.

In the key link of network information system security, human factor is also very important. Strengthening the ability and quality training of professional and technical personnel and popularizing the information security knowledge of business system userscan also make the computer and networkequipment in a more secure, stable, networks repeatedly.

The experiment is conducted to examine theperformance metrics of various networks such as AODV, T-AODV, SA-AODV and the proposed wireless sensor network.it isrepresented in the graph below. Time taken for route establishment and number of route discovery is conducted in which the proposed wireless sensor network is proved to be optimized technique. The experimentalresults are shown in the figure.2 below

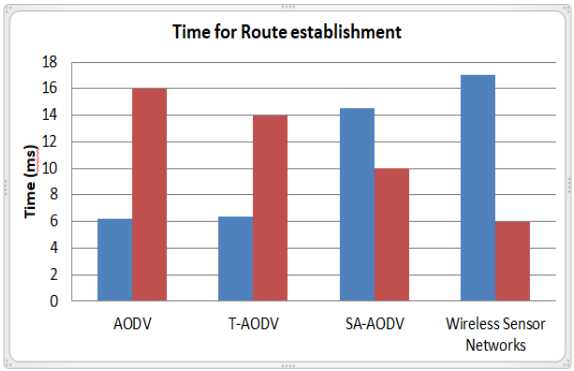

Fig.2: TIME TAKEN FOR ESTABLISHINGROUTES AND NUMBER OF ROUTE DISCOVERY.

From the above Fig.2 it is proved that the proposed WSN wireless sensor network has relatively reduced the number of threats overthe network which leads to enhancement of network security standard in a network area.

CONCLUSION

At present, the era of computer network is developing towards integration and diversification. While its increasingly complex system structure meets people's growing needs, the related security issuesare enough to attract people's attention. In this paper, a wireless network securityframework for protecting computernetworks is proposed. It integrates several collaborating security technologies to resist various types of attacks. It is a latest technology for detecting and to overcome the deceptive routing messages. The main concept of this paper is to develop a framework based wireless sensor network. Simulation tests show the ability of wireless sensor network (WSN) to provide security to the network against attacks and improve the network security

performance. Only by using practical security management means can the computer network information security management system be perfected and the security of user data can be guaranteed.

REFERENCES

1. Liu Haijiang, Jin Yong, Hu Zhentao, "Relay power allocation algorithm for wireless sensor networks in eavesdropping scenarios", High-tech Communications, vol.30, no. 2, pp. 150-156, 2020.
2. Feng Wei, Wang Feng, Xu Dan, "Joint secure routing and power allocation optimization algorithm for wireless sensornetworks", Journal of Sensor Technology,vol. 32, no. 4, pp. 610-617, 2020.
3. Yuan Hao, Mao Yingying, "Research onprivacy protection methods of node location in public mobile networks", Modern Electronic Technology, vol. 40, no. 16, pp. 35-37, IEEE Year: 2020.
4. Albagory Y, Said O., "Concentric Circular Arrays for Stratospheric High- Altitude Platforms Wireless SensorNetworks", Wireless PersonalCommunications, vol. 81, no. 2, pp. 1-13, 2019.
5. Ali R, Pal AK, Kumari S, "A secure userauthentication and keyagreement schemeusing wireless sensor networks foragriculture and monitoring", Future Generation Computer Systems, vol. 84, no. 6, pp. 200-215, 2019.
6. Chen Zhuo, Yang Qing, "Evaluation andanalysis of information security based on fish school neural network", China New Communications, IEEE Xplore, vol. 18, no. 015, pp. 111-112, Year: 2018.
7. Vartouni A M, Teshnehlab M, Kashi S
8. S. "Leveraging Deep Neural Networks for Anomaly-Based Web Application Firewall",IET Information Security, vol. 13, no. 4, pp. 352-361, 2017.
9. Suzuki Y, Kaneda Y, Mineno .H, "Analysis of Support Vector Regression Model for Micrometeorological Data Prediction", Gastroenterology, vol. 3, no. 2, pp. 37-48, 2015.
10. Xu Jun, "Application research of trusted computing mobile terminal based on biological characteristics trusted accessprotocol", Journal of Network and Information Security, vol. 3, no. 2, pp. 66- 76, 2014.
11. Deng Bin, Shi Zhidong, Fang Weidong,"Research on the secure multipath routing protocol for wireless sensor networks", Computer Applications and Software, vol.33, no. 11, pp. 263-268, 2013.
12. Zhou Wenqian, Wang Tao, Liu Jianlei, "Wireless sensor network synchronization acquisition system for impact test"Automation Instrumentation, IEEE vol. 38, no. 3, pp. 48-50+54, 2012.
13. I. Aad, J.-P. Hubaux, and E. W. Knightly, "Impact of denial of service attacks on ad hoc networks", IEEE-ACMTrans. Netw., vol. 16, no. 4, pp. 791–802, 2008.