Application of Big Data Technology in the Field of Communication Network Security

Ning Wang

Data Room of Comprehensive Support Center, Heilongjiang Provincial Corps of People's Armed Police, China
Email: 493252156@qq.com

Abstract. With the unceasing progress of science and technology, Internet technology has played a huge role in all walks of life, which changes people's production and living patterns. The application of big data technology has brought tremendous changes to the society, in recent years, the number of mobile communication users has been increasing day by day, and the structure of communication networks has become more and more complicated, which causes the network security risks to continue to increase, and communication network security is also facing a certain threat. In order to ensure the security of the communication network and create a good communication network environment, this paper studies the application of big data in the field of communication network security, and puts forward some specific application methods and development suggestions, aiming to provide some references for relevant research.

Keywords: big data, communication network, application.

1 Introduction

The communication network system is a system composed of communication equipment and relevant working procedures, which contains many types of communication methods, and its internal structure is very complicated. People's life, work and study are closely connected with the communication network; people's data and information are closely related to the security of the communication network, therefore, at present, the security problems of the communication network have aroused widespread concern of all walks of life, continuously improving the security of communication network is a very critical task in the current development of communication networks. In the era of big data, the importance of network communication security is more prominent, when facing the transmission of mass information; only by enhancing the reliability of communication network security can the value of big data be continuously exerted, moreover, big data also provides help for the construction of communication network security, therefore, it is of great significance to study the application of big data in the field of communication network security.

2 Communication Network and Network Security

The process of data transmission between the computer and the client usually uses telephones, optical fibers, or cables as transmission channels, which can make customers to share information; customers can process and modify the received information, this is the basic mode of data communication networks. Local area networks, wide area networks and international networks, etc., classify data communication networks based on the geographical location. The local area network can provide information transmission functions for enterprises and schools, and is widely welcomed for its stable network characteristics, it can also ensure the encryption of information, and can promote the improvement of the management efficiency and security of enterprises or schools.

With the advent of the era of big data, people are gradually transmitting more information on the network, and the network security problem has received widespread attention from society. Server terminals and nodes together form a network, ensuring the security of information and data transmission, and ensuring the stable operation of network systems are important tasks in network development.

3 Causes of Communication Network Security Risks

3.1 Complex Communication Network Structure

The communication network itself is a network with a complex structure, it is a system established organically with communication equipment and related working procedures, including multiple communication methods such as transmission, exchange, data, wireless mobile communication, microwave, satellite, and carrier wave. In recent years, the rapid development of the Internet industry has led to a new round of large-scale construction in the communications industry, which has formed a more complex communication network system, various problems occur during the operation of the established communication network system. On the other hand, due to the large number of standards in various types of communication equipment, the production and real-time control tasks carried by the equipment are heavy, and it is easy to cause many management negligence during the management process, and then there will be communication information security problems and cause various communication network security accidents.

3.2 Lack of Effective Data Analysis Methods

As the communication network continues to develop, people more and more rely on the network for communication and interaction, massive accumulation of data to be processed is the back-end of the network, which simply depends on the monitoring and processing of the back-end network management center, which brings great pressure to risk management of the communication network. On the other hand, because of the lack of efficient data analysis methods and analysis tools, communication network risk assessment mainly relies on the experience and judgment of analysts, which directly affects the accuracy and timeliness of the results of the assessment, make it difficult to ensure the timeliness and accuracy of network security risk assessment.

3.3 The Risk Assessment Method Needs to Be Improved

In addition to the complex communication network structure and various types of equipment mentioned, the operation of the communication network is also affected by external factors such as construction conditions, equipment environment and weather. If a communication failure occurs at the central office, various levels of alarms will appear in different network management systems, before the cause is finally determined, the monitoring personnel can only rely on manual analysis and notify the maintenance department to deal with it, which is slow and inefficient, it often delays valuable repair time. The reason is that the current risk assessment method does not conduct multi-dimensional analysis on the data of these equipment environments.

With the development of the communication industry, the structure of communication networks will become more and more complicated, and the analysis and evaluation data will increase exponentially, the existing security risk analysis methods are inefficient, heavy in workload, and inaccurate. Therefore, it is imperative to carry out improvement of communication network security risk assessment methods based on big data technology and ensure the security of communication networks under the new situation.

4 Big Data Technology and Communication Network Security Risk Identification

4.1 Big Data Technology

Big data is the abbreviation of big data technology, it is the massive, high growth rate and diversified information assets that require new processing models to have stronger decision-making power, insight and process optimization capabilities, its main content is to use various technologies to process scattered and huge amounts of information and data, and form valuable data and information through collection, management, analysis and processing, it is characterized by mass data scale, rapid data transfer, diverse data types and low value density.

4.2 Use Big Data to Identify Communication Network Security Risk

At present, the communication industry is forming a big data environment. In the process of identifying the security risks of communication networks, we must first pay attention to the development and application of big data technology, so that big data can be collected, analyzed, and processed. Secondly, in the research and development of big data technology, attention should be paid to multi-dimensional correlation analysis of data related to the communication network in order to comprehensively monitor the network operation status, realize automatic risk assessment of the communication network, fault-assisted judgment and warning.

5 Application of Big Data in the Field of Communication Network Security

5.1 Data Communication Technology

IP is a protocol for interconnection in networks; it is a protocol for computers to communicate with each other. It can clearly specify computer communication rules. The IP address is unique, which provides ideas for improving the security of communication networks. As a form of packet switching, data packets can segment the transmitted data into "packets" and then transmit them. It belongs to the "connectionless type", there is no need to connect a circuit before starting communication, and each data packet may not be transmitted through the same path. This feature of it can enhance the security of the network. The development of the Internet basic network and the advancement of Internet applications have promoted the development and maturity of IP communication technologies, enabling the construction of communications on new networks. Personalized communication and multimedia communication are two important aspects of communication needs. In addition, manageable converged communications is also an important direction. The convergence of IP communications and PSTN communications is an important way to improve the security of communications networks.

The key and encryption function prevent information from being recognized by others after the information is replaced or moved. This is the main application mode of data encryption technology and can play an effective role in the security of communication networks. The user's data is effectively protected by the conversion of plaintext information. The conversion method in the conversion of plaintext is the key. Cyclic redundancy check algorithm, cyclic shift, replacement table algorithm, improved replacement table algorithm and XOR operation algorithm, etc., are the main algorithm types of data encryption technology. Data encryption methods can be divided into symmetric encryption and asymmetric encryption. If the same key is used in the process of encryption and decryption, then this is symmetric encryption. The existence of data signatures greatly improves the security of data transmission. Data encryption standards include DES, 3DES, and AES. If the keys used during encryption and decryption is different, then this is asymmetric encryption. Cooperative decryption between "private key" and "public key" can effectively guarantee the security of information. The "private key" also has certain advantages in encryption speed and decryption speed.

5.2 Man-Machine Combination Tool

From the performance of system software and hardware transmission, analysis, storage, etc., it is an impossible task to extract content data, metadata and other information from the massive information. In order to meet the specific requirements of information extraction, technicians can achieve the extraction of information by verifying the structured extraction process of information, collecting the rolling cache of data, and collecting the key content of data, etc. To a large extent, the adverse effects of information collection, storage and other operations are minimized, but these methods cannot fundamentally solve all problems. However, the application of the man-machine combination tool in big data can effectively carry out unified analysis of multiple data. Therefore, technicians should actively use the man-machine combination tool and learn from some successful experiences abroad, so as to promote the man-machine combination tool to become more intelligent development.

In practical work, technicians in the field of communication networks should integrate the task models involved in the key areas with the corresponding workflows, and construct the application framework of man-machine combination tools through the construction of sensitivity analysis. Technicians need to

integrate information in technology, intelligence, etc., continuously improve information processing technology, enhance their ability to process information, always pay attention to the development trend and development direction of big data, and deeply understand the use of man-machine combination tools. In addition, the state should increase research efforts on man-machine combination tools, and increase investment in all aspects of man-machine combination tools research, with education as the basis, and cultivate more excellent talents in related majors. Only in this way can we alleviate the shortage of talents in the research field of man-machine combination tools, so that big data can be more conveniently applied in the field of communication network security.

5.3 Network Security

A complete communication network includes hardware and software. The hardware of communication network is generally composed of terminal equipment, transmission system and transfer exchange system, which are the physical entities of communication network. In order to make the whole network work harmoniously and reasonably, there are also various regulations, such as signaling scheme, various protocols, network structure, routing scheme, numbering scheme, tariff system and quality standard, which are all software. In a broad sense, network security refers to the use of various methods and defense means to ensure network security, including communication network security architecture, cryptography, security authentication and access control, network security technology foundation, wireless communication security overview, wireless communication security mechanism and other measures.

In the application of big data to network security, first of all, it is necessary to establish a communication resource network model and risk assessment algorithm, build a fault and risk analysis tool, establish a comprehensive security risk analysis system, analyze the communication network from multiple levels and dimensions, and take historical data, real-time operation data, fault statistics data, alarm information data and other system data as the big data Data source, using big data analysis and mining technology for network correlation analysis, to achieve online fault diagnosis, fault location analysis, intelligent alarm, intelligent early warning and other processing mechanisms; According to the network structure and operation mode, the network management is continuously optimized. At the same time, the equipment status and risk rules of the current network are combined to carry out dynamic evaluation on the equipment, find out the weak points of communication equipment and the high risk points of the system, and provide strong support for the analysis and judgment of later material procurement and risk identification.

6 Problems Needing Attention in the Application of Big Data in the Field of Communication Network Security

6.1 Strengthen Research on Behavior Models

If we want to make big data get more perfect application in the field of communication network security, we must strengthen the study of behavior models. In the field of communication networks, the application of big data is a very systematic work, it needs to be carried out under a relatively complete theoretical knowledge system, which requires technicians to conduct in-depth research on behavior models and changes data application method. Analysis of the entity model of big data in the field of communication network shows that the application of big data in the communication network focuses on putting big data in different types of entity behaviors, reconstructing a new network behavior model, and finally constructs a general framework of big data in applied theory. The entities mentioned here include physical entities and virtual entities. The entity objects studied by the more well-known communication network manufacturers are malware; they analyze the bad behavior of malware to identify the security threats in the communication network.

For the structured threat of malware to the communication network information, the national network department, private enterprises and individuals can submit the threat information to the country. After receiving the threat information, the country uses big data to manage it automatically, and makes an in-depth analysis of the attack mode of the threat information, and finally uses the automated method, all the information threatening the security of the communication network will be processed. Therefore,

according to the current situation of communication network, communication network technicians should increase the research on behavior model from the technical aspect, and actively encourage major communication network enterprises to explore and innovate big data, and strive to create a big data framework that meets the development needs, so that it can be more widely used in the field of communication network security.

6.2 Pay Attention to the Application of Information Extraction Technology

Entity behavior can be divided into three parts: entity forwarding, entity storage and entity production. In communication network, information mainly includes content data and metadata, and both of them are used to describe entity behavior. It can be called the foundation of big data application in communication network to extract the information of entity behavior in communication network and analyze it based on entity behavior model. It can be seen from the relevant research that the level of information extraction technology will have a certain impact on the analysis quality of entity behavior.

Normally, extracting content data and metadata will be related to address analysis, sender, language judgment, etc., and the newly developed information extraction technology has more extensive applications, for example, found in the communication network Information about the host that has been attacked by a hacker; collect information about Internet users in a browser; obtain the software's editing environment, author, and even author's coding habits based on the analysis results of MDS information. Edit author and editing environment, etc. With the help of various forms of extraction technology, information can be extracted more deeply and comprehensively, and behavior information sent by physical or virtual entities can be obtained. Then, technicians can aggregate addresses, contact chain hop by hop, etc. Different types of entities are grouped together. It can be seen that, in the context of the era of big data, the information extraction technology derived from big data can promote the development of a more secure trend in the field of communication networks. Therefore, technicians should increase the research on information extraction technology and enhance the level of information extraction technology, so as to improve the quality of analysis of entity behavior, which is also an important application of big data in communication networks.

7   Conclusion

With the continuous advancement of science and technology and the rapid development of the computer Internet, the era of big data has arrived. In the security management of communication networks, the application of big data technology has also received more and more attention. Therefore, it is necessary to gradually increase the analysis and research of big data technology to ensure that it plays a role in the security management of communication networks, thereby promoting the healthy development of the communication industry.

References

1. Li Yunong. Analysis on Application of Big Data in the Field of Network Security[J]. China Information Security, 2015.96-98.
2. Ye Lijia. Research on Information Communication Network Security Management Strategy under the Background of Big Data[J]. Digital Technology & Application, 2018, 36 (04): 178~179.
3. Xiong Gang, Lun Jieyong, Cao Xiaodong, Hu Guangxiong. Network Security Risk Criterion and the Application of Big Data[J]. Automation & Instrumentation, 2016(4):218-220.
4. Shan Qi. Thinking of Data Communication Network Maintenance and Network Security Problems[J]. Digital Technology & Application, 2017 (05): 215.
5. Guo Ning. Identification of Communication Network Security Risk and Analysis of Big Data Application[J]. Telecom World, 2016(9): 21.