Advances in Computer Science Research (ACRS), volume 54
International Conference on Computer Networks and Communication Technology (CNCT2016)

Research on the Cyberspace Security Evaluation Model of Smart City based on the Big Data Analysis Technology

Yuan TAO[1,2], Yu-xiang ZHANG[1,2], Ming LI[1,2] and Wen-rui MA[1,2]

[1]The Third Research Institute of Ministry of Public Security, China

[2]MPS Information Classified Security Protection Evaluation Center, China

Keywords: Big data analysis, Cyberspace security of smart city, Evaluation model

Abstract. In order to evaluate the cyberspace security of smart city, a new cyberspace security evaluation model of smart city is proposed, which is based on the big data and the classified protection technology. The key performance indicator and analysis algorithm is provided to quantify the cyberspace security of smart city, so that the effective information can be extracted from the large amount of security data, and the cyberspace security situation of smart city can be analysis and evaluated.

Introduction

Smart city is using new generation information technology[1], which contain Internet of things, cloud computing[2], big data[3], geospatial information integration[4] and other new information technology, so that urban planning, city construction, city management and service can be improved[5,6].

In order to promote the healthy and orderly development of smart city, cyberspace security of smart city should be assessment [7]. In this paper, a new cyberspace security evaluation model of smart city is proposed, based on combination of big data analysis and the classified protection technology. The key performance indicator and analysis algorithm is provided to quantify the cyberspace security of smart city, so that effective information can be extracted from the large amount of security data, and the cyberspace security of smart city can be analysis and evaluated.

The Cyberspace Security State of Smart City

More Serious Consequences of Cyberspace Attacks

The physical contact of smart city is more comprehensive, and the convenience is bring to the city users, but also cyberspace attack can be more easily carried out by hackers. For example, hackers can login Internet of things at any time and any place, and hackers can be very convenient using the cloud computing.

The malicious staff implementation of cyberspace attacks are becoming more extremely simple. If the operating system is controlled from Internet of things by hackers, the energy source of the target area will be complete controlled, including of water, electricity, oil, gas, transportation and other related systems. So that the economic lifeline of smart city is controlled by hackers.

Wider Range of Urban Important Information Resources

The most applications of smart city are running on the Internet, and a large amount of data are collected and stored from the Internet. The operation and management information of the city is including in these data.

The most information collection equipment of smart city are in unattended state, so that malicious personnel can steal the equipment to obtain the stored password and sensing data, and can attack through multiple copies nodes and radio interference signal. Hackers can also use the open application of smart city, which including cloud computing resources, to carry out big data calculation of confidential information.

The people of smart city can enjoy the convenience of interconnection, but facilities and articles of individuals and families are exposed on the Internet. In the construction of smart city, personal information is the core of big data. If the scale of personal information has be leaked, great distress and economic losses to the people will be cause.

Security Technology of New Application is Not Perfect

The construction of smart city is using virtualization and intensive cloud computing, perception and transmission of Internet of things, intelligent location services, massive data storage applications of new technologies and new applications. In addition to the usual information security threats will be face, the most typical security threats will be posed by the new technology and new application.

The security technology of cloud computing is not perfect: the traditional security protection mechanism is based on the physical security boundary, but virtual machine and virtual network cannot be effectively used these management, so the information security technology of user and application is difficult to effectively protect the virtual machine environment.

The security technology about the Internet of things is not perfect: the heterogeneity of the core network about the Internet of things has greatly increased the difficulty of security management. Because of the variety of data collected by the senser layer in the Internet of things, the data from various types of sensor nodes are massive and heterogeneous, so the security is more complex.

Cyberspace Security Evaluation Model of Smart City

Cyberspace Security Model of Smart City

Smart city is a new application mode, traditional security equipment or system is not very suitable for the application environment of this model, and the construction of applicable security protection equipment or system lags behind the construction of smart city.

The cyberspace security model of smart city is been construct in accordance with the classified protection and hierarchical prevention. The security guarantee of smart city is provided to protect important information systems and data resources. The security method includes management, technology, operation, evaluation and other aspects. The cyberspace security model of smart city is shown in figure 1.

The cyberspace security model of smart city includes 5 field: security of new technologies and applications, cyberspace security classified protection, cyberspace evaluation system, security protection architecture, operation and maintenance system of smart city.

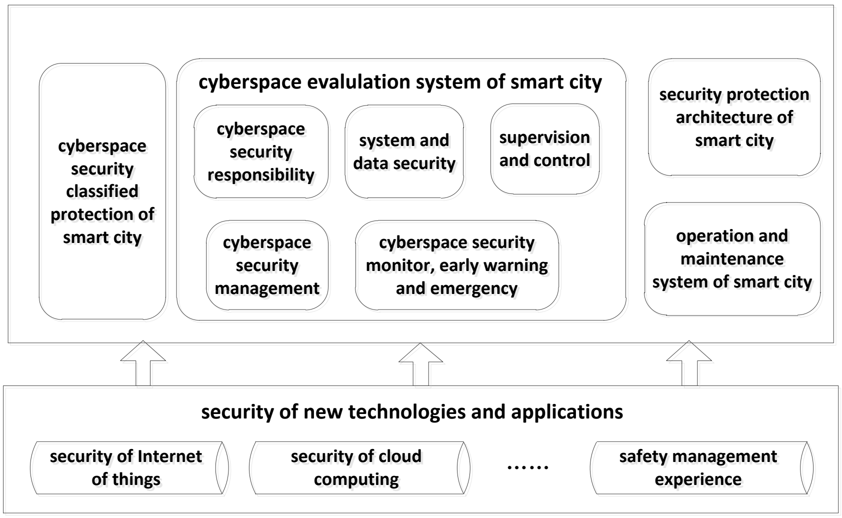
cyberspace security classified protection of smart city
cyberspace evalulation system of smart city
cyberspace security responsibility
system and data security
supervision and control
cyberspace security management
cyberspace security monitor, early warning and emergency
security protection architecture of smart city
operation and maintenance system of smart city
security of new technologies and applications
security of Internet of things
security of cloud computing
......
safety management experience

Figure 1. Cyberspace security model of smart city

Cyberspace Security Evaluation Model of Smart City

The cyberspace security evaluation model of smart city is proposed in this paper, which includes 5 field of cyberspace security. These 5 field are cyberspace security responsibility, cyberspace security management, system and data security, cyberspace security monitoring, early warning and emergency response, cyberspace security supervision and control of smart city.

The cyberspace security evaluation model of smart city is shown in figure 2.

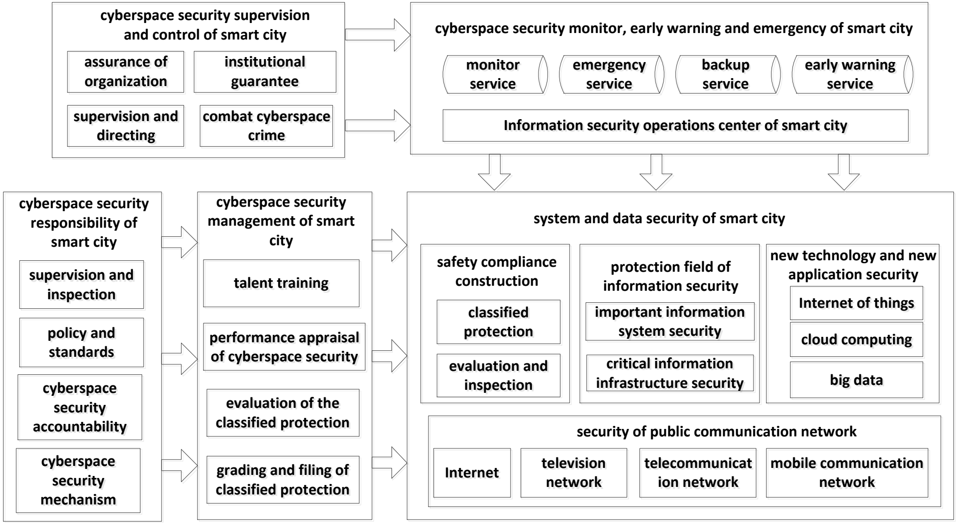
cyberspace security supervision and control of smart city
assurance of organization
institutional guarantee
supervision and directing
combat cyberspace crime
cyberspace security monitor, early warning and emergency of smart city
monitor service
emergency service
backup service
early warning service
Information security operations center of smart city
cyberspace security responsibility of smart city
supervision and inspection
policy and standards
cyberspace security accountability
cyberspace security mechanism
cyberspace security management of smart city
talent training
performance appraisal of cyberspace security
evaluation of the classified protection
grading and filing of classified protection
system and data security of smart city
safety compliance construction
classified protection
evaluation and inspection
protection field of information security
important information system security
critical information infrastructure security
new technology and new application security
Internet of things
cloud computing
big data
security of public communication network
Internet
television network
telecommunicat ion network
mobile communication network

Figure 2. Cyberspace security evaluation model of smart city

The core of smart city is composed of critical information infrastructure, important information systems and pivotal data source. The full range of smart city are enhanced by cyberspace security responsibility, cyberspace security management, cyberspace security monitoring, early warning and emergency response, cyberspace security supervision and control of smart city.

The Continuous Data Collection of Smart City

The continuous data collection of smart city is built on the Hadoop architecture. The bottom of the Hadoop is HDFS. It stores the date of smart city on all of the storage nodes in the Hadoop cluster. At the same time, HBase is running on the HDFS as a column oriented database. The goal of running HBase is to quickly locate the data needed for the billions of data in the host and access it.

MapReduce is used in order to deal with mass data of smart city. In order to mechanism for data tables and storage management services, HCatalog is used to provide a shared schema and data type.

In order to import data from the relational database to Hadoop, Sqoop is mainly used. Flume is used to directly to import the flow of data or log data into the HDFS. Zookeeper is used for coordinating the work process.

Map is used to get a set of key value pairs mapped into a new set of key value pairs. Reduce functions is specify concurrent to ensure that all the key of mapping each share the same set of keys. This process continues until the information is sufficiently simplified.

The Key Performance Indicator and Analysis Algorithm of Smart City

In order to extract effective information from the large amount of security data, the key performance indicator and analysis algorithm should be provided to quantify the cyberspace security of smart city, so that cyberspace security situation of smart city can be analyses and evaluated. The key performance indicator of cyberspace security is shown in table 1.

In table 1, the weight of KPI is defined as ω, and the score of categories is defined as C, so the cyberspace security score of the smart city is defined as S.

Table 1. Cyberspace security KPI of smart city

Categories	Key Performance Indicators	Weight	Score
cyberspace security responsibility of smart city	1)cyberspace security leadership of Smart city 2)cyberspace security mechanism of Smart city 3)responsible person of key information infrastructure and important information system 4)accountability system for major cyberspace security incidents	ω_1	C_1
cyberspace security management of smart city	1)Record rate of important information system 2)Record rate of critical information infrastructure 3)Record rate of information system evaluation	ω_2	C_2
system and data security of smart city	1)Classified evaluation score of important information system 2)funds guarantee of cyberspace security 3)Personnel training situation of cyberspace security 4)Performance implementation of cyberspace security	ω_3	C_3
cyberspace security supervision and control of smart city	1)Information sharing ability of cyberspace security 2)Information reporting and warning capability of cyberspace security 3)Emergency ability of cyberspace security 4)Disaster recovery ability of cyberspace security	ω_4	C_4
cyberspace security monitor, early warning and emergency of smart city	1)Inspection situation of cyberspace security 2)Guidance situation of cyberspace security 3)Cyberspace crimes situation 4)Combat situation of cyberspace crimes	ω_5	C_5

Critical information infrastructure is defined as CII, important information system is defined as IIS, important data resources is defined as IDR, Continuous data collection of smart city is defined as CDC, and the single score about cyberspace security of smart city is defined as C.

$$C = \frac{(CII + IIS + IDR) * CDC}{Intuitive \quad KPI} \tag{1}$$

The cyberspace security score of the smart city is calculated by the weighted sum method.

$$S = \sum_{i=1}^{5} C_i \omega_i \tag{2}$$

Conclusions

A new cyberspace security evaluation model of smart city is proposed. And the key performance indicator and analysis algorithm is provided to quantify the cyberspace security of smart city. The continuous data collection of smart city is provided by using big data analysis technology, so that the effective information can be extracted from the large amount of security data. So the cyberspace security situation of smart city can be analysis and evaluated.

Acknowledgement

This research was financially supported by the National Development and Reform Commission Information security special item “national engineering laboratory for key technology of classified information security protection”.

References

[1] Allwinkle S, Cruickshank P. Creating smarter cities: an overview. Journal of Urban Technology. 18(2), pp.1-16, 2011.

[2] Gregory S. Yovanof, George N. Hazapis. An architectural framework and enabling wireless technologies for digital Cities & intelligent urban environments. Wireless Personal Communications. 49(3), pp.445-463, 2009.

[3] Wang Yuan-Zhuo, Jin Xiao-Long, Cheng Xue-Qi. Network Big Data: Present and Future. Chinese Journal of Computers. 36(6), pp.1125-1138, 2013.(in Chinese)

[4] Deakin M, Al Waer H. From intelligent to smart cities. Intelligent Buildings International. 3(3), pp. 140-152, 2011.

[5] Mackey L, Talwalkar A, Jordan M I. Divide-and-conquer matrix factorization// Proceeding of the 25th Annual Conference on Neural Information Processing Systems(NIPS). Granada, Spain, pp.1134-1142, 2011.

[6] Li Guo-Jie, Cheng Xue-Qi. Research status and scientific thinking of big data. Bulletin of Chinese Academy of Sciences. 27(6), pp.647-657, 2012.(in Chinese)

[7] Akhilesh B. Sudha. R. IAIS: A methodology to enable interagency information sharing in e-Government. Journal of Database Management, 14(4), pp.59-80, 2003.