

Chapter 16

Evaluation of the Attack Effect Based on Improved Grey Clustering Model

Chen Yue

School of Information Technology and Network Security, People's Public Security University of China, Beijing, China

Lu Tianliang

Collaborative Innovation Center of Security and Law for Cyberspace, People's Public Security University of China, Beijing, China

Cai Manchun

Collaborative Innovation Center of Security and Law for Cyberspace, People's Public Security University of China, Beijing, China

Li Jingying

School of Information Technology and Network Security, People's Public Security University of China, Beijing, China

ABSTRACT

There are a lot of uncertainties and incomplete information problems on network attack. It is of great value to access the effect of the attack in the current network attack and defense. This paper examines the characteristics of network attacks, there are problems with traditional clustering that index attribution is not clear and the cross of clustering interval. A two-stage grey synthetic clustering evaluation model based on center-point triangular whitenization weight function was proposed for the attack effect. The authors studied the feasibility of applying this model to the evaluation of network attack effect. Finally, an example is given, which showed the model could evaluate the effect of the denial-of-service attack precisely. It is also shown that the model is viable to evaluate the attack effect.

DOI: 10.4018/978-1-7998-5348-0.ch016

1. INTRODUCTION

With the rapid development of modern computer technology, the dependence of people on the computer network is deepening. The network attack is the main way to tamper with people's networks, access to confidential information threatening the people's privacy and security. Because of the wide range of design and complex factors, the research of assessing the effect of network attack is a very important part of network attack and defense.

In 1982, Professor Deng had put forward the grey clustering method (Deng, 1982), which is widely used in many fields now, such as teaching evaluation, ecological evaluation and so on, which provides a great help for researchers. There are many uncertainties in the network attack bringing great difficulties to the evaluation work. The authors have improved the grey clustering method based on the selection of whitenization weight function and use it to evaluate the effect. At the same time, in order to solve the problem that traditional whitenization weight function has a certain overlapping in grey judgment that affects the result of evaluation, this paper proposed two-stage grey synthetic clustering evaluation model that based on center-point triangular whitenization weight function.

2. RELATED WORKS

2.1. Research on Network Attack Effect

The main research method of network attack effect evaluation is to evaluate the network attack effect through the designed model. Wang, Xian, and Wang (2005) presented a network effect evaluation model based on network entropy, which is based on the concept of entropy in information theory. In order to solve the problem of inaccurate data of some evaluation indexes, Cao, Zhang, and Wu (2009) proposed a network attack effect evaluation system based on fuzzy set, which makes the results more reasonable and effective. Wang, Jiang, and Xian (2009) proposed a method based on the attribute importance of rough set to reduce the subjectivity in the process of determining the weight of evaluation index. There is research work related to the effects of specific network attacks, such as denial of service attack and other evaluation methods (Wang, 2013) (Li, Zhang, & Zhu, 2015).

2.2. Research on Grey Theory

Grey theory is a kind of method to study the problem which has a little and uncertain information (Liu, 2014). Wang (2012) evaluated teachers' professional ability based on grey absolute degree to decide the rank of the teachers' professional training. Zhao, Zheng, and Zhao (2012) proposed an evaluation mode of the 3G network attack effectiveness based on AHP and grey relational analysis and use grey correlation analysis method to reduce the subjective effects brought by the AHP. Gao, Xu, and Wang (2011) used grey clustering to build a hierarchical network security evaluation system for power enterprises, and divided the network attacks into different levels through clustering. The evaluation system improved the display capabilities of the network security situation, and solved the human disturbance problem existed in the original system. Zhao (2013) presented a network protection capability evaluation model from information protection and defense to analyze the ability of target network protection. The application

7 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/evaluation-of-the-attack-effect-based-on-improved-grey-clustering-model/261984

Related Content

Strategic Communication for Supporting Cyber-Security

Tuija Kuusisto and Rauno Kuusisto (2013). *International Journal of Cyber Warfare and Terrorism* (pp. 72-79).

www.irma-international.org/article/strategic-communication-for-supporting-cyber-security/104524

The Security Aspects of Automotive Over-the-Air Updates

James Howden, Leandros Maglaras and Mohamed Amine Ferrag (2020). *International Journal of Cyber Warfare and Terrorism* (pp. 64-81).

www.irma-international.org/article/the-security-aspects-of-automotive-over-the-air-updates/250906

The Law Applicable to P2P Networks on National and International Bases for Violating Intellectual Property Rights

Ziad Kh. Al-Enizi and Muawya Naser (2022). *International Journal of Cyber Warfare and Terrorism* (pp. 1-10).

www.irma-international.org/article/the-law-applicable-to-p2p-networks-on-national-and-international-bases-for-violating-intellectual-property-rights/311419

Detection of Botnet Based Attacks on Network: Using Machine Learning Techniques

Prachi (2021). *Research Anthology on Combating Denial-of-Service Attacks* (pp. 74-88).

www.irma-international.org/chapter/detection-of-botnet-based-attacks-on-network/261971

Analysis of Possible Future Global Scenarios in the Field of Cyber Warfare: National Cyber Defense and Cyber Attack Capabilities

Flavia Zappa Leccisotti, Raoul Chiesa and Daniele De Nicolo (2016). *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare* (pp. 181-204).

www.irma-international.org/chapter/analysis-of-possible-future-global-scenarios-in-the-field-of-cyber-warfare/140522