Chapter 17

An Integrative Method for the Evaluation of Network Attack Effectiveness Based on Grey System Theory

Pengfei Wang
National University of Defense Technology, China

Wentao Zhao
National University of Defense Technology, China

Fan Zhang
National University of Defense Technology, China

Zimei Peng
National University of Defense Technology, China

ABSTRACT

On the basis of the grey system theory, which is proposed to tackle the problems of uncertainty and missing information, an integrative method for the effectiveness evaluation of network attacks is proposed, which combines the merits of three different kinds of evaluation methods based on Grey-Clustering Analysis (GCA). Particularly, the proposed method provides a solution to the problem of accuracy drop seen in prevailing grey evaluation methods when the clustering coefficients exhibit no significant difference. With low time complexity, the proposed method performs well in the effectiveness evaluation of network attacks. Simulation results on suitable DDoS scenarios demonstrate the feasibility and power of the method.

BACKGROUND

In the complex evaluation of network attack effectiveness, the key challenges can be attributed to the lack of data for evaluation, incomplete information and uncertainties. Proposed by Deng(2002) to tackle the problem of uncertainty and missing information, the grey system theory holds its inherent advantages in such evaluation. Three most common grey clustering methods include grey varied weights clustering, grey fixed weights clustering and grey clustering analysis.
An Integrative Method for the Evaluation of Network Attack Effectiveness

based on triangle whitening weight. They have been applied to multiple engineering fields such as the evaluation of the ability of knowledge management (Zheng & Hu, 2009), evaluation of military information network (Tang & Zhang & Su, 2008), system risk assessment (Ma, 2009), evaluation of attack effectiveness (Zou, 2011), and data mining (Liu & Dang, 2003). Although all of the three obtain the clustering results by comparing the coefficient vector of grey clustering, they apply grey clustering in different perspectives. The grey varied-weights clustering method is more suitable for problems with evaluation metrics close in meaning and dimension. For evaluations problems with indicators that have different metrics and large differences in magnitudes, improved methods should be considered.

The remaining parts of the work are organized as follows: related works are talked about in Section 2; Section 3 is the main thrust of the work, which includes the basic concepts of the grey systems theory, the description of the integrated grey clustering evaluation model and the experiments verification; Section 4 talks about the future trends of this work, followed by the conclusion in Section 5.

Wang, et al. introduced the grey system theory to the evaluation of network attack effectiveness and proposed a grey fixed weights grey clustering model and evaluation algorithms for the effectiveness of network attacks (Wang & Jiang & Xian, 2009). The grey clustering analysis employed in (Wang & Jiang & Xian, 2009) adopts the canonical method when assigning the grey class labels, which works by comparing the components of the grey clustering coefficient vector. The main disadvantage of such method comes from the ignorance of other components besides the maximum one. While in reality, it’s common to see no significant difference in clustering coefficients. The method described in (Wang & Jiang & Xian, 2009) will fail in such situations. To address this issue mentioned above, we propose an Integrated Grey Clustering Method (IGCM) for the evaluation of network attack effectiveness based on fixed-weight grey clustering analysis. Our method classifies the attack effectiveness into multiple categories that are determined by different evaluation metrics and whitening function of corresponding grey numbers. We add exponential components to the classical whitening function to deal with non-linearity for a better clustering result, and the time complexity for the whole algorithm is polynomial.

THE INTEGRATIVE METHOD FOR THE EVALUATION OF NETWORK ATTACK EFFECTIVENESS BASED ON GREY SYSTEM THEORY

Basic Concepts of Grey Systems Theory

Uncertainties are commonly seen in real-world problems. Statistical methods can be used if provided with a large amount of data. For those problems with much less data, one possible solution is the grey system theory. It does not require a vast amount of samples and the samples do not necessarily need to follow certain distributions. The number of samples in the evaluation of network attack effectiveness is usually small, which makes the grey system theory might be a feasible method.

1. Grey Number (Deng, 2002; Liu & Xie, 2008)

In complex systems, some parameters cannot be determined specifically but the ranges of their values are usually known. Grey number is a concept proposed to represent those parameters with ranges rather than exact values. In practice, grey number is the number of possible values in a range or a set, denoted as “⊗”.