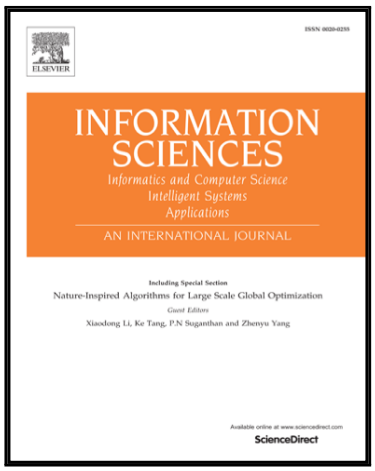

Measure of Invulnerability for Command and Control Network based on Mission Link

Wang Yunming , Chen Si , Pan Cheng-sheng , Chen Bo

PII: S0020-0255(17)31030-7
DOI: 10.1016/j.ins.2017.10.035
Reference: INS 13210

To appear in: *Information Sciences*

Received date: 17 April 2017
Revised date: 13 October 2017
Accepted date: 15 October 2017

Please cite this article as: Wang Yunming , Chen Si , Pan Cheng-sheng , Chen Bo , Measure of Invulnerability for Command and Control Network based on Mission Link, *Information Sciences* (2017), doi: 10.1016/j.ins.2017.10.035

Measure of Invulnerability for Command and Control Network based on Mission Link

Wang Yunming[1,2,*], Chen Si[2], Pan Cheng-sheng[2], Chen Bo[2]

[1]School of Automatic, Nanjing University of Science and Technology, Nanjing 210094, China,

[2]School of Information Engineering, Dalian University, Liaoning 116622, China

Abstract—In Command and Control (C2) network, the measure of invulnerability mainly focuses on structural characteristics of the network, where the operational mission has not been adequately considered. As a result, it becomes difficult to assess the invulnerability of C2 network in a dynamical manner. In this paper, the operational entities and heterogeneous relationships among combat entities are analyzed, where the operational C2 network model is constructed based on the combat theory of OODA and the super network. Subsequently, the mission link is defined, which can be used to characterize the combat network. Finally, a new measure of invulnerability for C2 networks is proposed based on the efficiency and entropy of the mission link. In particular, this measure can desirably represent the efficiency of information transmission and robustness of network structures, respectively. The simulation results have demonstrated that the proposed invulnerability measure is highly sensitive and accurate. More specifically, the proposed measure could more accurately reveal the invulnerability of C2 network, where theoretical basis for designing and optimizing the structure of C2 networks can be also provided.

Keywords—C2 Network, Invulnerability, Super Network Theory, Mission link Efficiency, Mission link Entropy.

1 INTRODUCTION

In information warfare, the C2 network plays an essential role in achieving superiority in information, which is helpful in decision-making process and will lead to better battle operations ultimately. On the one hand, C2 networks can connect the systems such as the early-warning detection system, the command and control system, and the firepower system etc. On the other hand, C2 networks can provide important guarantees for effective and synchronized operations [28]. The complex and diverse relationships among the elements of C2 networks have changed the major factors affecting the invulnerability for C2 networks, including the functionality and performance of elements and the system structure morphology of elements. However, failure of nodes or edges in C2 networks will often be caused by attacks, where the original network topology would become dividing and even lead to the damage of the global network [11]. If the C2 network is under attack, it remains to be an active research area to measure the invulnerability of C2 networks by evaluating the overall combat efficiency and complete combat mission[1,17].

Since the structure of C2 networks has transformed from the pyramid type to the type of flexible recombination and random access, various investigations have been performed for modeling network structures, invulnerability and robustness in C2 networks [29]. In general, the research of network invulnerability can be divided into two categories, i.e., graph theory and statistical physics. The graph theory based research primarily analyzed the invulnerability of the network, where measures including connectivity, toughness, integrity, tenacity, dispersion and nuclear were considered. These measures could be highly accurate; however, these methods were NP hard problems. Therefore, it is not even possible to apply these measures to large-scale C2 networks [36].The statistical physics base invulnerability measures were initially proposed by Albert [2]. The researchers have recorded the change of the network performance with removal of nodes or edges by various simulations of complex networks. In this way, the invulnerability of the network can be achieved. Based on this methodology, many researchers have evaluated the network performance from perspectives of information transmission efficiency and structural robustness [16].

These evaluation measures are based on the efficiency of information transmission including network diameter, average diameter, average path length, network efficiency and so on. Bian [3] has proposed an efficient algorithm for calculating the average diameter in the investigation of the minimum path graphs of directed double loop networks. In this work, the relationship between the network diameter and the average diameter was simulated. It has been concluded that the average diameter should be a better measure than the network diameter in evaluating the efficiency of network transmission. In [36], a class of algorithms were proposed to evaluate the network transmission efficiency. This method was able to effectively calculate the betweenness centrality and the average path length of a dynamic network. In [37], the efficiency of network was redefined to measure the efficiency of information transmission for multi-class network, where time-based decision criterion (TBDC)and monetary-based decision criterion (MBDC) standards were used to measure the validity and effectiveness of this index. Moreover, it was demonstrated that the index was very effective. In [38], a performance evaluation method was proposed, where Monte Carlo simulations were carried out based on network model to validate the reliability. In particular, a graph transformation based method was proposed to reduce the performance of protective measures, which could substantially reduce the complexity of network performance evaluation.

The structural robustness based on evaluation indexes mainly consist of the maximum connected subgraph, algebraic connectivity, natural connectivity and network structure entropy. In [18], a network robustness measure was proposed based on a maximal connected subgraph, where the robustness of networks was evaluated under all kinds of attacks, such as random attack, degree rank attack, betweenness rank attack. In [6], weighted algebraic connectivity was employed to analyze the robustness of

* Corresponding author

Email addresses: wang19871128@126.com (Wang Yunming), 1101903025@qq.com (Chen Si), pancs@sohu.com (Pan Chengsheng), chenbo20040607@126.com (Chen Bo)