

METRICS FOR NETWORKED SYSTEMS DESIGN IN A NETWORK-CENTRIC WARFARE CONTEXT

Vesa Kuikka¹

Abstract. This paper presents modelling techniques for networked systems. A network metric is suggested for evaluation and comparison of different networked systems in a network-centric warfare context with random or targeted attacks against the network structure. A method is also presented to calculate the threshold values of link failure probabilities where it is optimal for an attacker to shift targeted attacks against links of lower degree nodes. This information is vital for the defender in planning and constructing more robust networks against targeted attacks.

1. INTRODUCTION

This paper discusses modelling networked systems of services and users. Expressions for robustness are derived for realistic military situations. The methods are not limited to low failure probabilities so they are suitable for vulnerable and robust systems.

The goal of this paper is to develop a general framework for studying and comparing different networked systems when network links (edges) and nodes (vertices) become non-functional. The models presented here have a common viewpoint that one connection is enough for two parties to communicate, two connections are enough for three parties and so on. Here we use the term connection when there is a path between nodes—that is, connectivity is maintained. When all the nodes break down during the same time period, the system is down for the next time period. It is possible that during the repair period the nodes are destroyed again.

In the basic model, all the functional nodes in the system can do the same job. This is crucial when network metrics are calculated and makes a big difference to another definition of network metrics used in [6], where all the possible connections and nodes have been summed and weighted with values of links and nodes.

A networked system comprises three different elements: network links, functional network nodes, and technical network nodes. Functional network nodes are computer centres, command centres, users of networked services, and so on. Technical nodes are, for example, network routers and there are no applications for end users. Destroying a functional network node is usually more serious than destroying a technical network node. [7]

The framework consists of the following four steps:

- 1) Evaluate the failure probability p for a general target, a node or a link.
- 2) Evaluate the failure probability for a system of several nodes (Section 3).
- 3) Evaluate the failure probability for a network connection (several links) (Sections 4 and 5).
- 4) Evaluate the failure probability for a combined system of nodes and connections (Section 6).

In the first step the failure probability is evaluated for one target where firing theory is the tool if weapons are used against infrastructure [15]. Computer viruses and technical errors have to be taken into account by different methods. At the end of this step failure probabilities for functional nodes and links have been evaluated.

In step two, scenarios for one or several nodes are studied where, in the case of a node breakdown, a task transfer to another node can occur. The receiving node can be a standby node or a non-standby node. Task transfer to a standby node happens automatically and immediately after the failure. Task transfer to a non-standby node can occur after manual operations or rebuilding of the system. The main difference is that a transition to a standby node happens directly without delays and a transition to a non-standby node requires a preparation phase.

The goal in Section 3 is to construct a model sufficiently general to allow different modifications. The theory behind is discrete or continuous time Markov processes [5]. For Markov processes future states of the system are not influenced by the past of the system, only the current state is important. The limiting distribution is calculated as a first model but given the initial state, time dependence can be studied easily. Markov matrices serve also as a visualization tool for understanding the system's behaviour.

Step three is analogous to step two but the system is composed of network links. The probability for a connection between functional nodes is evaluated and a method is presented for the computation. Section 4 introduces some basic concepts of network connectivity. Section 5 presents a method to compute a measure of robustness for military networks or civilian networks under the threat of terrorist attacks. In the model attacks are not random but targeted so as to cause maximum damage to a network and unequal failure probabilities for network links are considered. Markov matrices or limiting processes are not used in Section 5 but the results can be utilized in Section 6 for limiting distributions. Alternatively, time-dependent solutions can be calculated by iterating waves of attacks with the methods of Section 5 alone.

In step four the system is regarded as a collection of functional nodes and links. The total failure probability for the system can be calculated. This is also a measure for comparing networks and networked systems. The survival probability of the system or the entire network is suggested as a new network metric (Equation (6.4)).

In the long run, if no repair takes place, the system will eventually break down. But if the number of spare parts or nodes is sufficiently large, compared to the time of hostile activity, the networked system can still operate until the end of the war. In this case the probability is fairly easy to compute. The probability distribution for the system in operation is given by the binomial distribution.

¹ Finnish Defence Forces, CIS Centre Development Division, Kutojankulma 2, PL 210, 02631 Espoo, Finland.