Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 107 (2017) 27 – 38

Procedia Computer Science

International Congress of Information and Communication Technology (ICICT 2017)

# Searching Forward Complete Attack Graph Generation Algorithm Based on Hypergraph Partitioning

Heng Li[a], Yongjun Wang[a], Yuan Cao[b, *]

*College of Computer Science and Technology, National University of Defense Technology, Changsha, 410073, China*
** Corresponding author:550551078@qq.com Tel.: 15574804153*

## Abstract

Attack graph is an effective method for network vulnerability analysis, existing methods of attack graph can't meet the requirements of the dynamical analysis of the large-scale complex network. In this paper, we proposed a searching forward complete attack graph generation algorithm based on hypergraph partitioning. First, ensure the load balancing of each of the computing agents by hypergraph partitioning; second, summarize various new attack templates; third, propose vulnerabilities exploited assumption, improve the efficiency of attack graph generation, reduce the recomputed work of attack graph generation dynamically; last, propose a new idea that generating the attack graph from the vulnerabilities to attacker reversely, ensure the integrity of vulnerabilities analysis, reduce the additional store memory and computing resources

*Keywords:* attack graph; dynamic; hypergraph partitioning; vulnerabilities exploited assumption;

## 1. Introduction

The rapid development of computer network communication technology has greatly changed the way people live. Network has been deep into every part of human life, so that humanity can break through the limitations of traditional space and time, which has brought to mankind greatly facilitate. However, the network convenient for people to live and work in greatly enrich the human world, but also brings security issues should not be underestimated。These security issues can be divided into two categories: external threats and internal vulnerabilities, of which the most fundamental reason is that internal vulnerability of the network system. Refers to the network of network vulnerability exists in the environment can be exploited by external factors, weaknesses or defects and thus constitute a hazard to the network environment, such as software vulnerabilities, protocol flaw, security policy conflicts[1]. If we get information about the vulnerability of the network, we use network vulnerability

doi:10.1016/j.procs.2017.03.052

analysis model describes the network environment, and analyze the relationship between vulnerabilities, which will be helpful to improving network security.

Attack graph is the most popular and effective method in existing network vulnerability analysis methods. From the attacker's view, attack graph enumerate all possible attack paths on the basis of the comprehensive analysis of network configuration and vulnerability information, helping defenders intuitively understand the relationship of vulnerabilities in target network and the relationship between vulnerabilities and network security configuration。As the size of network grows, the data need to processed increases, the memory space and computing time of the vulnerability analysis grows exponentially[2], so it is necessary to compute parallelly.

Existing attack graph construction algorithm mostly compute based on the data of a network at a time, there is no good way to assess the vulnerability of a network real-time. Most of existing algorithm builds the attack graph searching backwards from the attacker. The relevance of network vulnerabilities changes where the target network changes, we must recompute the attack graph if we want the correlation of the network vulnerabilities after the target network changed, but this way we can’t analyze the network vulnerabilities dynamically.

This paper presents a searching forward complete attack graph construction method based on hypergraph partitioning, to ensure that each computing agent parallel computing load balancing; Computing the complete attack graph in reverse direction from vulnerability nodes to the attacker; Reducing duplication of calculations in real-time attack graph constructed, being contributing to real-time analysis of network vulnerabilities while ensuring computational efficiency and accuracy

## 2. Related Work

At present, there are many ways to build the attack graph of large-scale network, which makes network security research has made great progress. According to the different meaning of the nodes and edges, attack graph is divided into two categories, one is state attack graph ,the main idea of state attack graph is: the advantage of the process of vulnerability network as the attacker's sequence of activities, according to the relationship of these sequences can generate a directed graph, this directed graph can show attack behavior and the method the attacker using .However, the scale of the attack path grows exponentially with the increase of the product of the hosts and the vulnerabilities, state attack graph can’t be applied to large-scale networks. Another one is attribute attack graph, the main idea is: attack graph nodes represent atomic attack and attribute nodes, attribute nodes represent premise or consequences of atomic attack graph, to reflect the trajectory of the attack implicitly[3]. This is convenient to analyze the source of attack, such as TVA[4]、MulVAL[5-6.] Practice indicates that attribute attack graph has good scalability, it can be applied to large-scale network, our prototype system also uses the attribute attack graph.

To simplify the attack graph generation, improve the efficiency of attack graph generation, solve the combinatorial explosion when generate attack graph, Ammann[7] al. Introduce “monotonic” hypothesis to attack graph model firstly, namely, that attackers continue to expand their capabilities without losing the ability which attackers have acquired during the attack .In China ,attribute compression, attack template filter and instantiation inspection proposed by ChenFeng[8] et al. also increase efficiency. However, with the scale of network increases, the existing methods can’t meet the performance requirement of large-scale network vulnerability analysis.

HuXin[9] et al. proposed an attack graph generation method of parallelization based on the assumption network security grads attack in 2011. He use network security grads to show the importance of different nodes, and proposed method to calculate the network security grads in static or dynamic. Static network security grads measures network grads based on firewall rules and network topology; Dynamic network security grads measures based on network traffic. The assumption of network security grads attack that attacker will not attack from high network security grads segments to low network security grads segments, namely, attacker will not attack from the high-value network nodes to low-value network nodes, which is in line with the actual network. The generation and analysis of attack graph increase efficiency and reduce complexity based on grads monotonicity constraint. In subsequent studies, we found that, although the method of grads hypothesis greatly improve the computational efficiency, but also make attack graph missing some attacks that may occur between the vulnerabilities in the process of attack graph generation; Meanwhile, the generation and analysis of attack graph based on the network security grads hypothetical did not care about the network information changed except traffic information, namely,