ON-LINE DETECTION OF DISTRIBUTED ATTACKS FROM SPACE-TIME NETWORK FLOW PATTERNS

J.S. Baras*, A.A. Cardenas, V. Ramezani
Electrical and Computer Engineering Department
and the Institute for Systems Research
University of Maryland
College Park, MD, 20742

ABSTRACT

Parametric and non-parametric change detection algorithms are applied to the problem of detecting changes in the behavior of network traffic that may be due to distributed attacks. Detection of spreading active code and of distributed denial of service attacks are investigated. Novel formulations and algorithms are developed and investigated including detection of changes in the "direction" of traffic flow. The performance of our change detection algorithms is evaluated via simulations.

1. INTRODUCTION

We are interested in detecting and classifying anomalous changes in the behavior of a network caused from distributed sources of the disturbance, including maliciously planned attacks with goal the disruption of the network. More specifically we are interested in detecting changes in the network flow, identifying abnormal changes, and extracting the characteristics of the changes, as soon as possible. Examples include the spreading of active worms through web servers, email viruses and distributed denial of service attacks.

We investigate first the problem of a spreading congestion attack that incrementally compromises nodes. The behavior pattern as observed by different nodes in the network will be different from a panic mode (flash crowd). This problem is investigated as a step towards analyzing more complex distributed attacks. Various techniques have been proposed for mitigation of denial of service attacks that require the identification of the routers participating (involuntarily) in the attack. We are addressing this monitoring and detection of abnormal behavior problem as a space-time inference problem.

More specifically for the denial of service attack problem, we use a "directionality" framework, which gives us a way to compute the severity and directionality of the change. The "severity" represents a composite hypothesis test that can be solved explicitly when the data are Gaussian. We also introduce a heuristic distributed change detection mechanism for "correlating" the alarms in a subset of monitored nodes.

2. DETECTION OF SELF-PROPAGATING CODE

Our overall goal is to develop automated mechanisms for detecting worms (self-propagating code) based on their spread traffic patterns from widespread sensors (later attacks). Recent studies, have revealed on a preliminary basis, that graph topology, and in particular its classification from the perspectives of clustering coefficients and degree distribution, is intimately related to the robustness of the network when there is failure or attack. There are strong indications that scale free networks are very robust to random failures but susceptible to targeted attacks, while ad hoc networks are very robust to targeted attacks. Figure 1 below, illustrates a typical scale-free network. In such a network the distribution of the node degree is heavy tailed, meaning that there is higher than typical chance that there are some nodes with many edges connected to them. Such nodes help spread attacks rapidly and are themselves primary targets of attacks. The network of Internet routers and the WWW are well known examples of such networks.

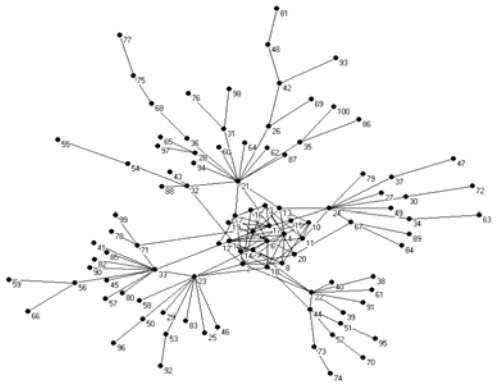

Figure1: The synthetic experimental network

3. CHANGE DETECTION IN A NETWORK FLOW PATTERN

We take a new approach for identifying Distributed Denial of Service (DDoS) attacks by a set of nodes in a transit network. The basic idea is that at each highly

connected node, the data tends to aggregate from the distributed sources towards the destination, giving a sense of "directionality" to the attack. This directionality concept provides us a framework to design change detection algorithms that are going to be less sensitive to changes in the average intensity of the overall traffic and will focus in differentiating the different random fluctuations of the network traffic versus fluctuations where there is a clear change in the direction of the flow at a given node.

One of the main advantages in having several nodes under monitoring is that we can perform a correlation of the statistics between the different nodes in order to decrease the detection delay given a fixed false alarm rate probability. The alarm correlation can be performed by several methods. Here we propose a simple algorithm that will only require the knowledge of the routing tables for the nodes being monitored.

For our experimental results we used the network simulation software ns2. We created a script to generate a random scale-free (Albert and Barabasi, 2002) transit network topology with a given number of sub networks. It consists of 15 transit nodes performing only routing between 12 subnetworks, each with 65 hosts each. The attack is simulated with a given number of compromised nodes in different sub networks. During the attack, each of these nodes will start a constant bit rate connection towards a specific node. The rate of the attackers was varied to test the detection algorithm with different percentage of attack packets circulating over the transit network at a given time. We considered 7 attackers. One in each of the sub networks connected to nodes 3, 4, 5, 8, 9, 11 and 13. The victim is in the network connected to node 14.

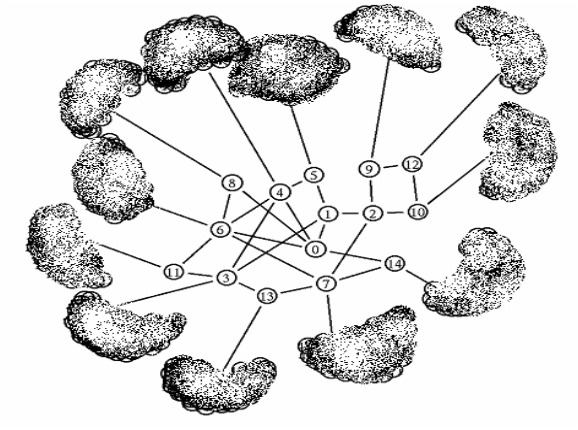

Figure 2: The transit network consists of 15 routers. Each "cloud" represents a subnetwork

Not only can we detect the attack (depending on the new correlation threshold), but also we can diminish the impact of the false alarms. Another important conclusion is that without the need to extract or store header information from the packets transmitted through the network, we are able to infer (from the intersection of the two routing tables for the "winning" correlated statistic of links possible targets of an attack.

CONCLUSIONS

In this paper we have investigated the problem of detecting anomalous behavior and distributed attacks in a network. We investigated detection of spreading of active code based on the spatio-temporal pattern variations in the flows of a set of nodes. We also investigated detection of distributed denial of service attacks. We have formulated these problems as distributed change detection problems on a graph. We described several algorithms and their performance.

ACKNOWLEDGMENTS

This material is based upon work supported by the U.S. Army Research Office under Award No. DAAD19-01-1-0494 to the University of Maryland College Park.

REFERENCES

Albert, R. and Barabasi A.-L. "Statistical Mechanics of Complex Networks," Reviews of Modern Physics,pp. 47-97, January 2002.

Basseville, M. and Nikiforov I.V. *Detection of Abrupt Changes: Theory and Application*, Englewood Cliffs, NJ: Prentice Hall, 1993.

Blâzek, R.B., Kim H. Rozovskii B. and Tartakovsky A. "A novel approach to detection of denial-of-service attacks via adaptive sequential and batch-sequential change-point detection methods," IEEE Systems, Man and Cybernetics Information Assurance Workshop, June 2001.

Bohacek, S., "Optimal Filtering for Denial of Service Mitigation," IEEE Conf. on Dec. and Control, 2002.

Houle K.J and Weaver, G.M. "Trends in Denial of Service Attack Technology" CERT Coordination Center v1.0 October 2001.

Shiryaev, A.N., *Optimal Stopping Rules*, Springer, 1978.

Staniford S., Paxson V. and Weaver N. "How to 0wn the Internet in your Spare Time," Proceedings of the 11th USENIX Security Symposium (Security '02) 2002.

Wang, H. Zhang D. and Shin K.G. "Detecting SYN Flooding Attacks," Proceedings of INFOCOM 2002, New York City, New York, June,2002.