Seton Hall University

From the SelectedWorks of Manfred Minimair

Spring March 5, 2018

Network Analysis for Malware Intrusion Detection

Davis Cook
Wilbert Chagula
Bianca Reilly
Abbey Sterner
Joshua Talamayan, et al.

Available at: https://works.bepress.com/minimair/33/

Network Analysis for Malware Intrusion Detection

Davis Cook, Wilbert Chagula, Bianca Reilly, Abbey Sterner, Joshua Talamayan, Catherine Way
Advisor: Dr. Manfred Minimair
Seton Hall University
Department of Mathematics and Computer Science

Project Supported by Comcast Innovation Fund

Motivation Malware Intrusion Detection

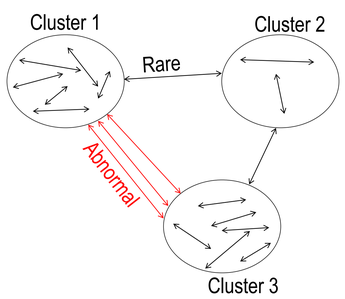
We were motivated to do this project because in current society, network security is becoming more and more necessary. Each week you hear on the news about a new intrusion in a large company so we need to find a way to make sure that our network is secure.

Anomaly Detection Procedure

The network being analyzed is a company network

Objectives:

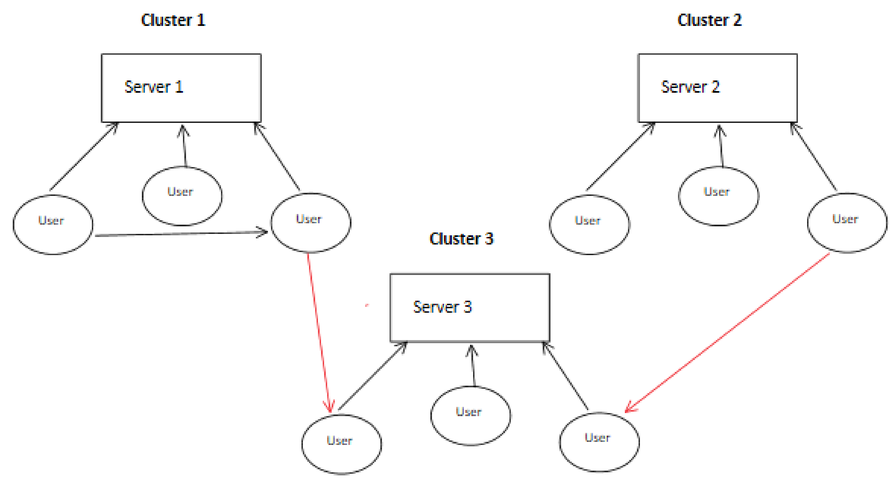
1. Observe the network to find out the usual number of clusters. We suppose that there should be a prevailing number of clusters because we are dealing with a small network.
2. Determine communication probabilities to match the parameters from the network simulator.
3. Determine the ideal time frame for observation of unusual activity.



Network Data Sources

- Network Simulator at Seton Hall
- Internet

Network Analysis Objectives



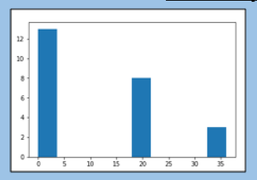
Each user connects to the server and can occasionally go to the other users in the same cluster. An **unusual connection** would be if a used from one cluster connected to a server or user from a different cluster. Our **objective** is to find a way to define and be able to identify what an unusual connection is.

Network Analysis

Steps Taken:

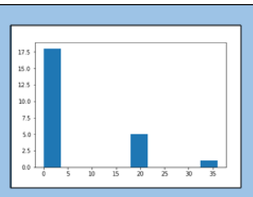
1. *Networks were simulated* by forming clusters of users that tend to behave in similar ways on the network. Examinations were begun by looking at only 2 clusters.
2. *Communication data was collected* – this included the probabilities that users in a cluster would communicate other users in the cluster or to users in the other cluster.
3. *Distribution style was examined and defined* – Based on connections formed, a pattern was defined in the communications among clusters
   - Number of connections between different clusters per a predetermined time frame were counted (every 5 seconds)
   - Investigation of number of connections and connection patterns

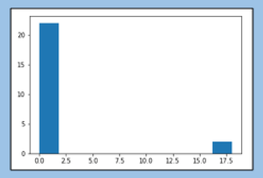
Cluster type: 1 server, 1 user



"clusters2":
Cluster 0: to cluster 1 with probability 0.1
Cluster 1: To cluster 0 with probability 0.1

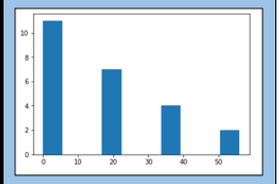
"cl2rare":
Cluster 0: to cluster 1 with probability .02
Cluster 1: to cluster 0 with probability .02
Both clients can send simultaneously





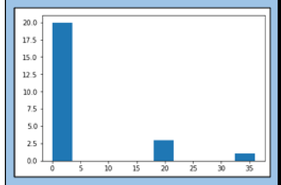
"clusters2rare":
Cluster 0: to cluster 1 with probability of 0.02
Cluster 1: to cluster 2 with probability 0.02

Cluster type: 1 server, 2 users



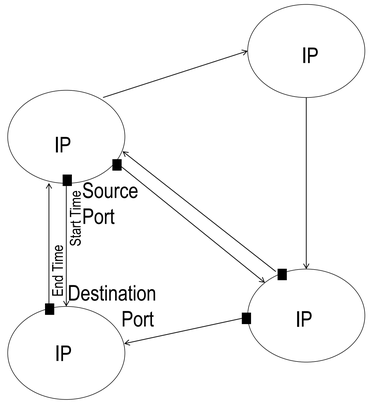
"cl2":
Cluster 1 : To cluster 1at probability 0.1
Cluster 0 : To cluster 0 at probability 0.1

"s1c1_s1c1":
Cluster 0: client only sends to the server in its cluster.
Cluster 1:
to Cluster 0 with probability 0.1.



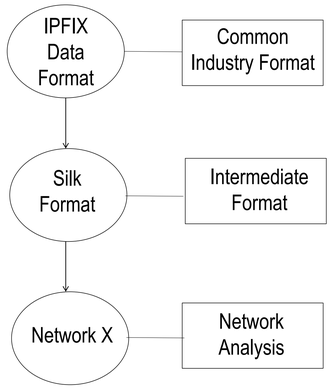
Researchers hoped to find a normal distribution in the data, but as example data was analyzed, a considerably steady decreasing pattern was found. With more data examples, researchers hope to conclude the data resembles the right hand side of a normal, bell-shaped curve.

Data Import Module



The goal of the Data Import Module is to make the network data easily accessible with Python.

Python Module



Import network data into Python for analysis.

Ongoing Work

- Import more Data Formats (Argus, Konect)
- Release as an open source project

www.PosterPresentations.com