July 11, 2018

TARGETED NETWORK ANOMALY DETECTION

Martin Grill

Martin Kopp

Jan Kohout

TARGETED NETWORK ANOMALY DETECTION

AUTHORS:
Martin Grill
Martin Kopp
Jan Kohout

ABSTRACT

Techniques are described herein for clustering network hosts based on their network behavior to create groups of hosts that behave similarly. An anomaly detection model trained on a single group of network hosts is more robust to fluctuations of the behavior of individual hosts when compared to the per host models. When comparing to the group all models that are trained using the behavior of all network hosts, finer anomalies (e.g., stealthy data exfiltration) that would otherwise be hidden may be detected by modelling diversely behaving network hosts.

DETAILED DESCRIPTION

Network behavior anomaly detection (NBAD) systems are complementary to the traditional network security systems based on deep packet inspection (DPI). Contrary to DPI, NBAD can detect new zero-day attacks (i.e., attacks without known signatures) and work even with encrypted traffic. As a result, NBAD adoption continuously grows. NBAD systems detect threats by tracking various network characteristics in real time and maintaining a model of a “normal” (i.e., baseline) behavior. Every new observed behavior is then compared against the baseline and any deviation that could indicate the presence of a threat generates an alarm. Therefore, the quality of the result depends heavily on the quality of the baseline: the better the baseline, the finer the anomalies that can be detected.

Traditionally, there are two main approaches to generating the baseline of the normal behavior: modelling per host and modelling for the whole network. The per host model typically suffers from only a small amount of noisy input data as the behavior of a single user is typically not very stable. The model for the whole network is typically much more robust to the fluctuations of the behavior of the individual network hosts, but suffers from the fact that the baseline model is trying to determine the normal behavior of a group of hosts of diverse behavior.

Accordingly, described herein is a method of creating groups of network hosts based on their behavior in the network that are then treated separately by an anomaly-based detection system. This allows significantly more precise models of normal behavior (baseline of the anomaly detector) of the individual groups, which leads to a higher recall of the whole anomaly detection system when compared to the anomaly models updated by the network traffic.

Figure 1 below illustrates the effect of this grouping. The effect of grouping is analyzed on a single specific anomaly detection method that is monitoring the amount of data transferred in the observed network. The first graph (A+B) shows the amount of transferred data over a period of six days for all network hosts. As can be seen there is no clear anomaly in the traffic. If the network is separated into smaller groups based on the host behavior, the individual components of the A+B graph may be obtained as A and B. When the A and B groups are modelled separately, a clear anomaly is represented by the sudden increase of activity in the case of group B. The individual per group anomaly detection models still have enough data to be able to create sufficient baselines, and since the baseline is built only from the groups of hosts with consistent behavior, much finer anomalies may be detected.

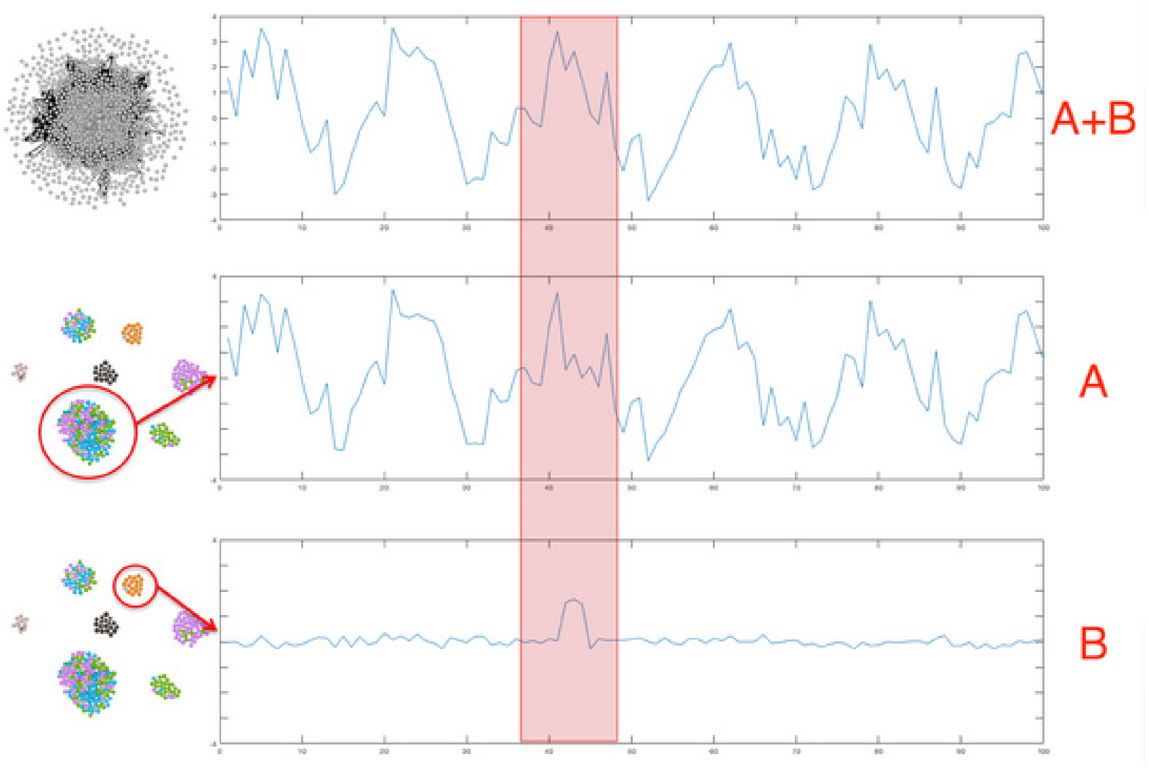
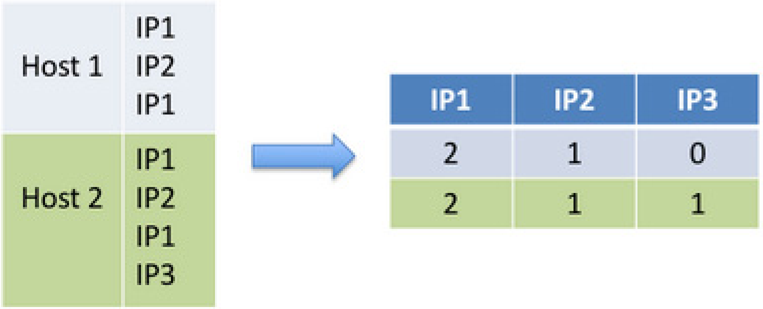


Figure 1

To divide network hosts into groups, network traces (e.g., indications sent from network monitoring applications, web access logs, etc.) may be analyzed in a predefined time window (e.g., 24 hours).

Each network host may be represented by a histogram of frequencies of individual feature values. The features may be used by the monitored network host and may include server hostname, server Internet Protocol (IP) address, server IP address and server port, application identifier (as parsed by firewalls), user-agent, string (for web access logs), process hash, etc. For example, if the feature is the server IP address, a histogram may be constructed for each host such that it contains all server IP addresses that were contacted by the host in last 24 hours. As illustrated in Figure 2 below, the size of the histogram bin may be defined by the frequency of the usage of that particular feature value (e.g., frequency of server IP address visits).



Host 1	IP1 IP2 IP1
Host 2	IP1 IP2 IP1 IP3

IP1	IP2	IP3
2	1	0
2	1	1

Figure 2

The frequency may be calculated as ratio of the number of time slots in which the specific server IP address was contacted by the host to the total number of time slots in which the host was active. This is a relatively robust representation.

To cluster the network hosts into groups, a similarity graph may be built where nodes represent the internal network hosts. At first the graph may be a fully connected graph, where the weight of an edge is defined by the cosine similarity of the above defined histograms that represent the behavior of the hosts. The low similarity edges may be pruned to emphasize homogenous groups and reduce the computational complexity. The hosts may be clustered using the Modularity clustering algorithm (also known as Graph community detection) that identifies densely connected groups.

Targeted anomaly detection uses the above-defined groups to create a baseline model for every group separately. To ensure that there is sufficient data to generate the baseline, only clusters that have more than ten network hosts may be considered. The hosts that belong to small clusters may be handled by the fallback anomaly detection model, which uses all internal network hosts to generate the baseline. Experiments show that more than 80% of internal network hosts are covered by larger clusters. The anomaly detection algorithm may be based on different algorithms and use different features analyzing time series, empirical probabilities, etc. To demonstrate the effect of the grouping, the precision-recall curve of anomaly detectors that model the empirical probability of autonomous systems of the server IP address were evaluated. For the evaluation, 11,000 recent malware samples were used. As illustrated in Figure 3 below, the targeted anomaly detection approach described herein outperforms both the per host and all network anomaly detection methods.

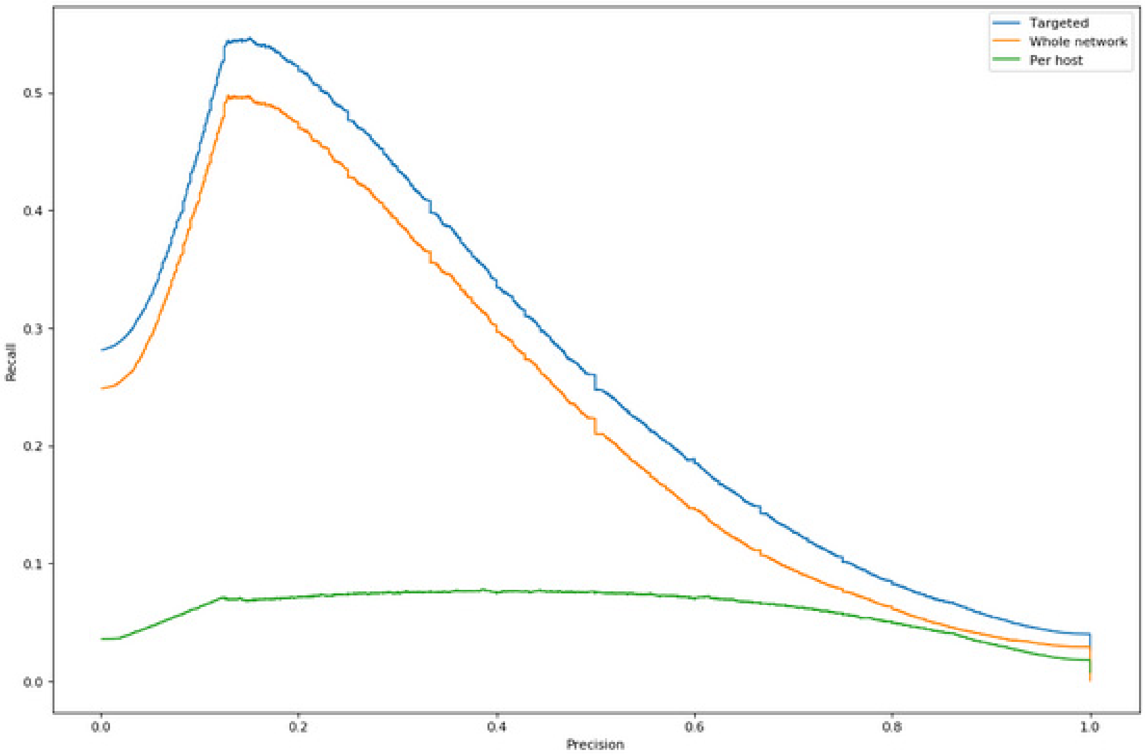


Figure 3

Figure 4 below illustrates anomaly detector per host cluster against anomaly detector based on all hosts.

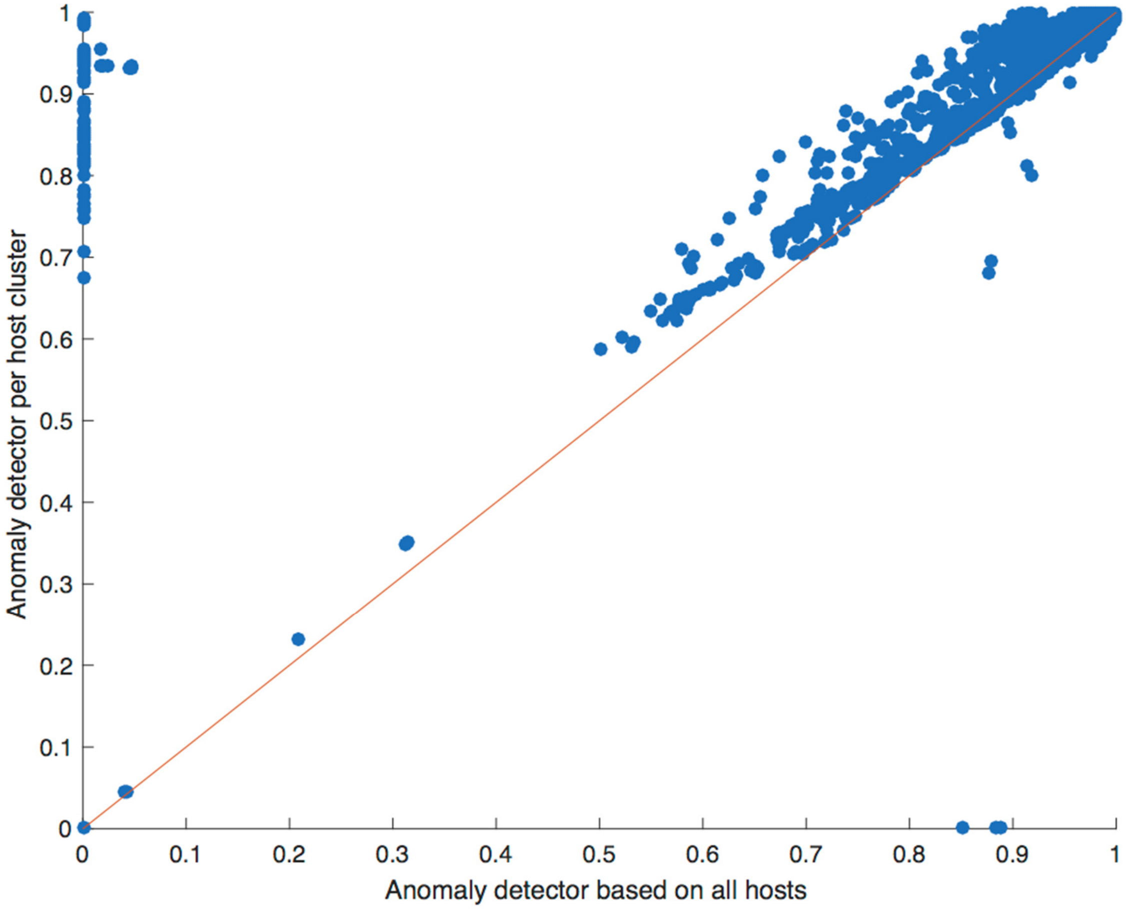


Figure 4

In summary, techniques are described herein for clustering network hosts based on their network behavior to create groups of hosts that behave similarly. An anomaly detection model trained on a single group of network hosts is more robust to fluctuations of the behavior of individual hosts when compared to the per host models. When comparing to the group all models that are trained using the behavior of all network hosts, finer anomalies (e.g., stealthy data exfiltration) that would otherwise be hidden may be detected by modelling diversely behaving network hosts.