Unsupervised Network Anomaly Detection

Miss Nita V. Jaiswal, Prof. D.M. Dakhne

ABSTRACT:

In this paper we present a completely unsupervised approach to detect attacks, without relying on signatures, labeled traffic, or training. The unsupervised detection of network attacks represents an extremely challenging goal. The structure of the anomaly identified by the clustering algorithms is used to automatically construct specific filtering rules that characterize its nature, providing easy-to-interpret information to the network operator. In addition, these rules are combined to create an anomaly signature, which can be directly exported towards standard security devices like IDSs, IPSs, and/or Firewalls.

Keywords—Unsupervised Anomaly Detection & Characterization, Robust & Distributed Clustering, Automatic Generation of Signatures, Autonomous Security, Evidence Accumulation, Outliers Detection, Abnormality Ranking.

INTRODUCTION

In this paper we present a completely unsupervised method to detect and characterize network attacks, without relying on signatures, training, or labeled traffic of any kind. Our approach relies on robust clustering algorithms to detect both well-known as well as completely unknown attacks, and to automatically produce easy-to-interpret signatures to characterize them, both in an on-line basis. The analysis is performed on packet-level traffic, captured in consecutive time slots of fixed length and aggregated in IP flows. IP flows are additionally aggregated at different flow levels. These include (from finer to coarsergrained resolution): source IPs, destination IPs, source Network Prefixes, destination Network Prefixes and traffic per Time Slot.

The complete detection and characterization algorithm runs in three successive stages. The first step consists in detecting an anomalous time slot where an attack might be hidden. For doing so, time series are built for basic traffic metrics such as number of bytes, packets, and IP flows per time slot. Any generic anomaly detection algorithm based on time-series analysis [1]–[6] is then used on time series to identify an anomalous slot. The unsupervised detection and characterization algorithm begins in the second stage, using as input the set of IP flows captured in the flagged time slot. In the third stage, the evidence of traffic structure provided by the clustering algorithms is used to produce filtering rules that characterize the detected attack and simplify its analysis. The characterization of an attack can be a hard and time-consuming task, particularly when dealing with unknown attacks.

The principal challenge in automatically detecting and analyzing traffic anomalies is that these are a moving target. It is virtually impossible to precisely define the set of anomalies that may arise, especially in the case of network attacks, because new attacks as well a new variants of already known attacks are continuously emerging. A general anomaly detection system should therefore be able to detect a wide range of anomalies with diverse structure, using the least amount of previous information, ideally no information at all.
Two different approaches are by far dominant in current research literature and commercial detection systems: signature-based detection and anomaly detection. Signature-based detection is the de-facto approach used in standard security devices such as IDSs, IPSs, and firewalls. When an attack is discovered, generally after its occurrence during a diagnosis phase, the associated anomalous traffic pattern is coded as a signature by human experts, which is then used to detect a new occurrence of the same attack. Signature-based detection methods are highly effective to detect those attacks which they are programmed to alert on. However, they cannot defend the network against new attacks, simply because they cannot recognize what they do not know.

UNADA runs in three consecutive steps, analyzing packets captured in contiguous time slots of fixed length. Figure 1 depicts a modular, high-level description of UNADA. The first step consists in detecting an anomalous time slot in which the clustering analysis will be performed. For doing so, captured packets are first aggregated into multi-resolution traffic flows. Different time-series are then built on top of these flows, and any generic change-detection algorithm based on time-series analysis is finally used to flag an anomalous change. The second step takes as input all the flows in the time slot flagged as anomalous. In this step, outlying flows are identified using a robust multi-clustering algorithm, based on a combination of Sub-Space Clustering (SSC) [10], Density-based Clustering [2], and Evidence Accumulation Clustering (EAC) [11] techniques. The evidence of traffic structure provided by this clustering algorithm is used to rank the degree of abnormality of all the identified outlying flows, building an outliers ranking. In the third and final step, the top-ranked outlying flows are flagged as anomalies, using a simple thresholding detection approach. As we will show throughout the paper, the main contribution provided by UNADA relies on its ability to work in a completely unsupervised fashion, outperforming previous proposals for unsupervised anomaly detection.

**EXPERIMENTAL EVALUATION**

We evaluate the ability of UNADA to detect different attacks in real traffic traces from the public MAWI repository of the WIDE project [12]. The WIDE operational network provides interconnection between different research institutions in Japan, as well as connection to different commercial ISPs and universities in the U.S.. The traffic repository consists of 15 minutes-long raw packet traces daily collected for the last ten years. The traces we shall work with consist of traffic from one of the trans-pacific links between Japan and the U.S.. MAWI traces are not labeled, but some previous work on anomaly detection has been done on them [7, 13]. In particular, [13] detects network attacks using a signature-based approach, while [7] detects both attacks and anomalous flows using non-Gaussian modeling. We shall therefore refer to the combination of results obtained in both works as our ground truth for MAWI traffic.

We shall also test the true positive and false positive rates obtained with UNADA in the detection of flooding attacks in traffic traces from the MET-ROSEC project [14]. These traces consist of real traffic collected on the French RENATER network, containing simulated
attacks performed with well-known DDoS attack tools. Traces were collected between 2004 and 2006, and contain DDoS attacks that range from very low intensity (i.e., less than 4% of the overall traffic volume) to massive attacks (i.e., more than 80% of the overall traffic volume).

For example, we could use the set of traffic features generally used in the traffic classification domain [19] for our problem of anomaly detection, as this set is generally broader; if these features are good enough to classify different traffic applications, they should be useful to perform anomaly detection. The main advantage of UNADA is that we have devised an algorithm to highlight outliers respect to any set of features, and this is why we claim that our algorithm is highly applicable.

Fig.: Detection and analysis of network attacks in MAWI.

We shall begin by analyzing the performance of UNADA to detect network attacks and other types of anomalies in one of the traces previously analyzed in [7]. IP flows are aggregated according to IPsrc key. Figure .(a) shows the ordered dissimilarity values in D obtained by the Evidence Accumulation for Ranking Outliers(EA4RO) method, along with their corresponding manual classification. The first two most dissimilar flows correspond to a highly distributed SYN network scan (more than 500 destination hosts) and an ICMP spoofed flooding attack directed to a small number of victims (ICMP redirect traffic, directed towards port 0). The following two flows correspond to unusual large rates of DNS traffic and HTTP requests; from there on, flows correspond to normal-operation traffic. The ICMP flooding attack and the two unusual flows are also detected in [7]; the SYN scan was missed by their method, but it was correctly detected with accurate signatures [13].Figures .(b,c) showing typical characteristics of the attacks, such as a large value of nPkts/sec or a value 1 for attributes nICMP/nPkts and nSYN/nPkt respectively, both figures permit to appreciate that the detected attacks do not necessarily represent the largest elephant flows in the time slot. This emphasizes the ability of UNADA to detect attacks of low intensity, event lower than normal traffic.

RELATED/ PROPOSED WORK

Most approaches analyze statistical variations of traffic volume-metrics (e.g., number of bytes, packets, or flows) and/or other traffic features (e.g., distribution of IP addresses and ports), using either single-link measurements or network-wide data. A non-exhaustive list of methods includes the use of signal processing techniques (e.g., ARIMA, wavelets) on single-link traffic measurements [1], [3], PCA [7], [9] and Kalman filters [5] for network-wide anomaly detection, and sketches applied to IP-flows [4], [7]. Our approach falls within the unsupervised anomaly detection domain. Most work has been devoted to the Intrusion Detection field, targeting the well known KDD’99 data-set. First and most important, it works in a completely unsupervised fashion, which means that it can be directly plugged-in to any monitoring system and start to work from scratch, without any kind of calibration or previous knowledge. Then takes as input all the flows in the time slot flagged as anomalous, and apply sliding time windowing scheme for every 1sec and extract the number of sources and number of destination, number of bytes etc. Creation of feature space matrix by using following formula
x(1) = [sip dip sp nsip/ndip y(1)/ndip ]Similarly, we have to create feature space matrices for all time windows data set.

i.e., X=∑(x1,x2…….xn)

and then apply Clustering algorithm and declare smallest group of cluster as outlier. Combine the feature space and flow of data Then find out the abnormal data by using the K-means-type algorithm. From that abnormal data we have to gather the information about srIP, DesIP and time for that we have to trace back into feature space matrix, aggregation and log file .We will have all information regarding anomalies data transact. Use trace data to Create signature for anomalous flow. Signature will be logged and updated the signature table. Signature table can be use for online detection anomalous flow.

CONCLUSION

The main advantage of our unsupervised approach relies on the fact that this new signature has been produced without any previous information about the attack or baseline traffic, and now it can be directly exported towards any security device to rapidly detect the same attack in the future.

The completely unsupervised algorithm for detection of network attacks. It uses exclusively unlabeled data to detect and characterize network attacks, without assuming any kind of signature, particular model, or canonical data distribution. This allows detecting new previously unseen network attacks, even without using statistical learning. By combining the notions of Subspace Clustering and multiple Evidence Accumulation, the algorithm avoids the lack of robustness of general clustering approaches, improving the power of discrimination between normal-operation and anomalous traffic. The use of the algorithm for on-line unsupervised detection and automatic generation of signatures is possible and easy to achieve for the volumes of traffic that I have analyzed.

REFERENCES:-