Classification of transport layer data using Multi-way Association Clustering Analysis

Sheneela Naz[1], Sohail Asghar[1], Simon Fong[2], Amir Qayyum[3]
[1]Center of Research in Data Engineering (CORDE),
Mohammad Ali Jinnah University, Islamabad, Pakistan
shahneela.cs@gmail.com, sohail.asghar@jinnah.edu.pk
[2]Department of Computer and Information Science,
University of Macau, Macau SAR
ccfong@umac.mo
[3]Center of Research in Networks & Telecommunication (CoReNeT),
Mohammad Ali Jinnah University, Islamabad, Pakistan
aqayyum@ieee.org

ABSTRACT: *Currently, the categorization of real time multicast data using payload-based analysis is producing practical limitations with many applications that a network supports. Through this work, we set our goal to identify the recurrent patterns and classification of transport layer data, as an effective measure of anomaly-based intrusion detection. We have identified them by using association rules techniques such as Apriori and clustering algorithms. The evaluation experiment was carried out to test the efficacy of the algorithms. We are able to find an association between flow parameters for network traffic from the simulated data. We advocate that the current study contributes a possible approach of analyzing behavior patterns for building a network traffic intrusion detection system and firewall at Transport layer, by using unsupervised association rule mining and clustering techniques.*

Keywords: Transport Layer Data, Multi-way association, Clustering, Association rules, Real-time multicast, Network security

Received: 17 November 2010, Revised 21 December 2010, Accepted 29 December 2010

1.Introduction

A large variety of malicious attacks against computer network communication can be generally categorized into three aspects [1]: attacks against confidentiality, attack against integrity and attack against availability. The last two aspects of attacks (against confidentiality and against integrity) can be protected by manipulating the data with secrecy such as data encryption and data digestion methods; whereas attacks against the availability of a vulnerable computer network can be detected through the use of intrusion detection systems. Intrusion detection systems mainly function by two approaches on recognizing the users' behaviors, such as misuse detection and anomaly detection. Misuse detection tries to detect previously known attacks and flag the matching patterns. It assumes history of the attack is already known. In anomaly detection it checks on the network traffic behavior and measures how much it deviates away from the normal network behavior. Anomaly detection is useful at detecting abnormal usage and it requires no prior knowledge on this new attack.

Multi-way Association Clustering Analysis on Adaptive Real-Time Multicast Data (MACAA) is an anomaly-based intrusion detection system (IDS) that uses a combination of association rules and clustering methods to identify malicious computer network activity from the traffic data. There are number of association rules techniques available in literature; e.g. they are Apriori, filtered associations and predictive Apriori, and clustering techniques are K-means, Y-means, DBSCAN etc.

Several techniques have been used in the past to classify network traffic flow. Jeffrey Erman et al. [2] classified network traffic

by inspecting a list of Transport layer characteristics through the implementation of unsupervised approach such as clustering. The variables of Transport layer characteristics consist of duration of connection, total number of packets sent, size of packets and number of bytes sent. For network traffic classification (segmentation), K-Means and DBSCAN clustering algorithms are used in this paper. The results of these two algorithms are also compared with those by another clustering algorithm AutoClass. The performance of these three algorithms are studied together for identifying the pros and cons. Accuracy wise AutoClass algorithm performs very well, better than the other two clustering algorithms. K-Means and DBSCAN algorithms run quicker than AutoClass. As observed from the results of this performance evaluation, for network traffic classification K-Means algorithm seems to be more suitable other than the other two algorithms because its accuracy is relative high and its model building time is efficient. It takes approximately only one minute for model building where as DBSCAN takes approximately three minute and AutoClass takes approximately four and half hours in our experiments.

2. Background

There are a number of various techniques used to detect the anomalies in network traffic. According to Animesh Patcha et al. [4] mainly there are three types of techniques: statistical techniques, data-mining based methods, and machine learning based techniques. They are summarized in Figure 1.

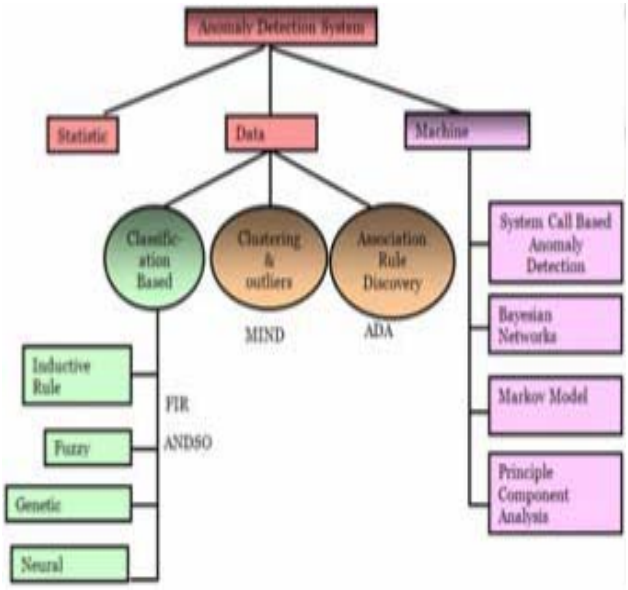

Figure 1. Anomaly detection techniques

In statistical techniques, statistical measurements are used to reveal anomalies.Some well-known statistical anomaly detection techniques are Haystack [5], NIDES [6], Staniford et al. [7], and Ye et al. [8]. Data mining-based anomaly detection systems are largely built upon the following categories of techniques: Classificationbased Clustering plus outlier detection and association rule discovery. Some examples of data mining-based anomaly detection systems are MINDS [9], ADAM [10] and FIRE [11] etc. Machine Learning category can be further branched into four subcategories which are system-call based, anomaly detection, Bayesian networks, and Markove model and principle component analysis. Some machine learning based anomaly detection techniques are PHAD [12], ALAD [13] and Valdes et al. [14] etc.

In [1], Umang et al. proposed a network flow classification framework that performs two main tasks. First, it performs classification of network traffic, and second, it conducts the application behaviors profiling. Supported network traffic types by this framework include TCP, UDP and ICMP for wired or wireless data classification that was enabled by unsupervised clustering algorithms. This machine learning classification model contains three processes. They are Clustering, Transductive Classification technique and Association Rule Classification. These machine learning processes accept the flow data as input and perform the clustering on input flow data using K-Means and Modeling based clustering algorithms. After the clustering process is done, the next process Transductive Classification technique follows. The labels of the clusters are assigned. Then Association Rule Classification is applied for each cluster, then it proceeds to the final classification of given data flow as output. In this process Association Rule algorithm such as Apriori is applied. Under this framework, performance comparison

between K-Means and Model based clustering algorithms with association rule techniques was model. The comparison shows that performance of K-Means is inefficient while Model based clustering performs efficiently and it also supports detection of new network traffic patterns.

The study exposed some short-comings of K-Means clustering algorithm which are the dependency and degeneracy of the number of required clusters. These two short comings are overcome in the work of Yu Guan et al [3]. Yu Guan et al proposed an intrusion detection clustering algorithm called Y-Means. The following steps describe the functional flow of Y-Means algorithm: partition the input data of total size n into k clusters where k lies between 1<k<n. After that, check a condition whether there is any empty cluster or not. If there are empty clusters then replace them out with newly created clusters. This process is repeated until there is no empty cluster remains. At the end the clusters are labeled according to the ratio of the instances. If the ratio is above a predefined threshold value, then these instances are labeled as normal; otherwise they are intrusive. Two major advantages can be found in Y-Means clustering algorithm; first is that it creates automatically an appropriate number of clusters, and second is raw log data can be used directly as training data without the need of labeling.

Founded on the Y-Means algorithm and its merits, Yu Liu et al proposed a hybrid technique which is used to detect the node based anomaly for ad-hoc communication networks [15]. This anomaly detection is considered as a hybrid approach that combines two data mining techniques. Associations rule mining techniques and crossfeature mining techniques are used together in action. This hybrid method takes two feature sets which are direct feature set and statistical feature set of MAC layer data and network layer data respectively. Direct feature set targets on short-term node behavior profiling and statistical feature set targets on long-term node behavior profiling. For short-term profiling, this method applies associations rule mining techniques and for long-term profiling it uses cross-feature mining techniques. Fig 2 shows the feature set taxonomy according to this paper [15].

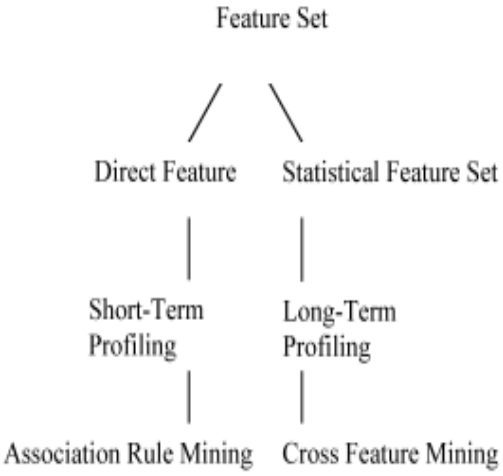

Figure 2. Feature set taxonomy

Direct feature set of MAC layer is used to locate the source of attack within one hop perimeter. In that paper, multiple attack sources are evaluated through the Bayesian networks. The result analysis of both data mining techniques proves that the proposed IDS are effective because association rule provides precise detection performance whereas cross-feature approach is energy-efficient and effective in monitoring the network behavior.

Some classification based anomaly detection methods used the network traffic to detect the anomaly [11, 16, 17]. J. E. Dickerson et al. uses fuzzy logic to detect the malicious activity on network traffic such as TCP, UDP and ICMP data [11]. This technique is anomaly based intrusion detection system which is called Fuzzy Intrusion Recognition Engine (FIRE). This technique uses network input data features as fuzzy sets. These sets are used to define fuzzy rules. So, these rules can help to detect the individual attacks.

Several machine learning techniques are also used for anomaly detection in network traffic. Nong Ye proposed an anomaly diction technique which is used Markov chain model to detect intrusions attempting to hack into network systems. This

technique represents the normal profile of temporal behavior. Probability is used to infer the normal behaviors and anomalous behaviors. If the probability is low then it implies the pattern is of anomalous behavior otherwise it is normal.

Another machine learning technique is used for host based anomaly intrusion detection. It processes sequences of system calls which form a multi layer intrusion detection model [18]. Their results indicate that this approach performs better in terms of accuracy and response time to detecting anomalous behavior of the software programs. This method is thus suitable for online intrusion detection.

For evaluation purposes we have used two protocols, one is Adaptive Smooth Multicast Protocol (ASMP) and second one is Packet-pair receiver-driven cumulative Layered Multicast (PLM). These protocols are multicast congestion control protocols
and which are commonly applied over the transport layer. The trace files of these protocols were collected for analysis. Some descriptions of these protocols are defined below.

3. Multicast Congestion Control Protocols

Congestion control protocols play a pivoted role in reliable transfer of data in computer network. There are number of multicast congestion control protocols. We have selected two multicast congestion control protocols for simulation. We shall elaborate both of them briefly.

3.1 Adaptive Smooth Multicast Protocol (ASMP)

ASMP was initially coined by [19]. It is a single-rate multicast transport protocol which is used for multimedia data transmission. It runs on top of UDP/RTP/RTCP protocols. In ASMP, sender and receiver share current information about network conditions through the use of RTCP sender and receiver's reports. In sender driven congestion control protocols, sender adjusts its transmission rate. ASMP is the sender driven protocol, so ASMP sender adjusts its sending rate according to the receiver's feedback reports. Receiver's feedback reports contain the receiving rate, as described in [20] which is calculated at each receiver according to the TCP analytical model.

Each receiver measures the following values such as packet loss rate, Round Trip Time, Delay Jitter and Congestion Indicators (CI),using the early congestion indication algorithm before the calculation of new TCP-friendly transmission rate. After calculating the current transmission rate, each receiver sends it to the sender by using the RTP/RTCP extensions. So, the sender receives the newly calculated receiving rate through receiver's feedback report and then it adjusts the sending rate keeping in consideration to the slowest receivers in the session. The main features of this protocol are: Smooth transmission rates, TCP-friendly behavior, and High bandwidth utilization. An advantage of this protocol is that it does not require any additional support from the routers or the underlying IP-multicast protocols. A disadvantage of this protocol is that, it does not show a very responsive behavior in varying network conditions because the gap between two successive RTCP feedback reports is very long.

3.2 Packet-pair receiver-driven cumulative Layered Multicast (PLM)

Packet-pair receiver-driven cumulative Layered Multicast (PLM) was proposed by [21]. It is meant to address some deficiencies of Receiver Driven Layered Congestion Control multicast protocol (RLC). It is the multirate multicast congestion control protocol which is used for multimedia data transmission, such as, live audio/video. It runs on top of UDP/RTP protocols. In receiver driven congestion control protocols, the receiver is responsible for adapting the video transmission rate by subscribing and unsubscribing through various protocol layers. Therefore Receiver has an active role while the sender has a passive role in adapting receiver based rate control. PLM is the receiver based congestion control mechanism, so the congestion control algorithm is implemented at the receiver side. Whereas at the sender side data is transmitted via cumulative layers and each layer packets are sent out in pairs. PLM defines two basic mechanisms: Receiver-side Packet-pair Probe (PP) and Fair Queuing (FQ).Receiver-side Packet-pair Probe (PP) mechanism is used to estimate the currently available bandwidth and Fair Queuing (FQ) mechanism is used at each router. PLM assumes fair scheduler network and deploys a fair queuing mechanism at routers. It relies on a fair scheduler to ensure fairness, including intra-protocol fairness, interprotocol fairness and TCP friendliness. PLM has some advantages over RLM and RLC. RLM and RLC produce losses at joint attempts, whereas PLM does not suffer any loss in discovering the available bandwidth. It has a fast convergence for rate adaptation.

4. Performance Evaluation

The input log files that are to be used in the performance evaluation experiments aregenerated by a simulation program NS2.

The simulation is configured with multicast congestion protocols ASMP and PLM.

4.1 Simulation Setup and Topology

For the sake of the simulation-based experiments, ns simulator version 2.33 was used and integrated with the available code of PLM (built-in) and ASMP (asmp V1.1). Simulation topology was created in the NsWorkBench (nsBench v1.0) environment.

Figure 3. shows the topology which was designed for checking the fairness and responsiveness of these two protocols. The bottleneck link from R1 to R2 has bandwidth of 600 Kbps and time delay of 8ms. Interior links from R2 to R3, R2 to R4 and R2 to R5 have 10Mbps bandwidth and delay of 8ms each. All exterior links have 10Mbps bandwidth and delay of 8ms. Each simulation trial was run for 250 seconds. Data rate of TCP and UDP connection is set at 500Kbps. Initially data rate for multicast protocol is 500Kbps. There is one multicast session (ASMP/PLM) and three TCP/UDP connections in total.

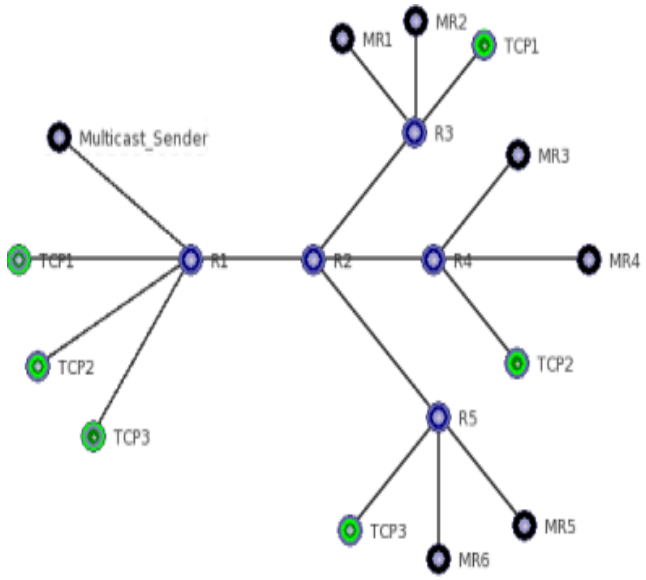

Figure 3. Simulation Topology

4.2 Feature of Interest

Transport layer data is rich in a variety of intrinsic features. Interested features from the perspective of the experiment are extracted from the Transport layer protocols which are used to multicast the multimedia data such as Adaptive Smooth Multicast Protocol (ASMP) and Packet-pair receiver-driven cumulative Layered Multicast (PLM) which are run over the UDP protocol. In PLM/ASMP trace file, there are three packet types such as data, prune and graft. Data packet contains the multimedia data. The proposed feature set and its value space is illustrated in Table 1.

Simulation experiment yields trace file of large number of recordset. Data mining community is well aware of the fact that piles of data are prone to yield useful information. However in order to extract useful patterns, it is a mandatory requirement to perform data preprocessing activity. Researchers have argued that preprocessing activity normally consumes much of the time of overall experiment and the same was true in our case. The trace files essentially contain records of data packets that traversed across the specific links in the network topology and the patterns of these accesses are shaped by the specified protocols along those links. This processed trace file/log file is used as input to the data mining process unit in which the data mining algorithms are implemented.

Figure 4 outlines the flow of data mining process model. It consists of multilevel association rule mining and clustering technique. Association rule is a supervised learning technique while clustering is a unsupervised learning technique. Association rule mining discovers the hidden relationships among the data which are sometimes known as casual relations. Multilevel association rule mining unit is driven by Apriori algorithm. The data mining unit reads in the input trace files and creates a

Feature	Feature Value
Flow Direction	Send, Receive, Drop
Source Address (SA)	One/many
Destination Address (DS)	One/many
Traffic Type	CBR/UDP, RTP/UDP,TCP
Packet Type	DATA, Prune, Graft
Sending Rate	Bytes
Packet Id	Number
Sequence #	Number
Time	Seconds

Table 1. Feature Set

number of association rules by using Apriori algorithm. Data of the features of interest that occurred frequently together in the access records are sorted out. This sorted data is identified as association rules.

The next step is extracting the association rules from the trace files; the process classifies these extracted rules into groups according to their semantic meanings by applying K-Means clustering algorithm. This unsupervised clustering technique groups together association rules with the criteria of similar characteristics.

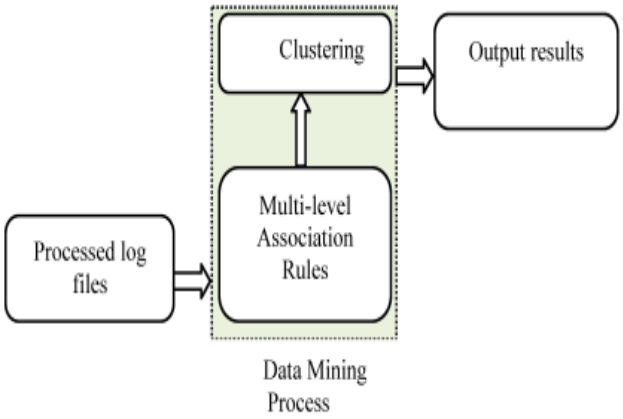

Figure 4. Data Mining Process Model

5. Multilevel Association Rules

Multilevel association rule mining is aimed towards discovering the relations between data items at multiple levels in a given dataset. The data is subjected to normalization process with formats of RTP, UDP and TCP protocols. Multilevel association rules have the provision to recognize the pattern of computer network traffic while building a set of heuristic rules for prediction. According to the features of interest given in table 1, a transaction record is an artificially synthetic instantiation of the following feature set:

{Flow direction, SA, DA, traffic type, packet type, sending rate, pktid, seq#, time}

The rules shown in the table 2 have been generated using the orange tool.Where SA, DA stands for Sender Address and Destination Address.

An example association rule looks like this:

HEAD (rec=multicast) ← BODY (Type=cbr, packetsize=500, fid=1).

For cbr, packet is received on the multicast address. This packet size is of 500 units so is quantified as 500 only. cbr packet type and flow id is 1 with support of 18 and confidence of cbr packet type and flow id is 1 with support of 18 and confidence of 1.0. When we track back this rule, we are accurately able to classify this rule as the cbr packet.

Packet Type	Rule	C.	Lift	Str.	Cov	Leverage
TCP	Type=tcp → pktsize=540	1.0	4.414	1.000	0.227	0.175
RTP	Type=rtp → pktsize=1000	1.0	4.412	1.000	0.225	0.175
ACK	Type=ack → pktsize=40	1.0	4.430	1.000	0.226	0.175
CBR	rec=multicast → Type=cbr, pktsize=500, fid=1	1.0	2.238	1.184	0.377	0.209

Table 2. Apriori Based Association Rules

Each rule is associated with the following performance parameters [22] that might indicate how interesting or significant the rules are: Lift indicates the strength of the rule because it defines the ratio of the probability that antecedent and consequent occur together. Confidence is the number of cases in which the rule is correct relative to the number of cases in which it is applicable.

Rules with lower value of confidence, lift, leverage, strength and coverage are filtered out. This leaves only the most important rules which are ranked and appeared on the top in descending order. Fig. 5 shows the taxonomy of packet in a hierarchical representation. This representation which is a rooted tree represents the type, packet size, receiving status and flow id at first level. In the next level packet type is split into cbr, tcp, rtp and ack whereas packet sizes is grouped into 500, 540 and 40. Flow id is branched out into numeral values 1, 2 and 3. Packet receiving status is further branched out into multicast etc. These branches can be further divided into number of branches. Fig. 6 represents the multi-way association rules. Conceptually both of them are same in implantations.

6. Clustering Analysis

The clustering in data mining is a well renowned technique for grouping similar objects. In literature various algorithms and techniques have been discussed and proposed. In our proposed architecture we have used K-Means clustering. K mean clusters are based on a variety of measures including manhitten distance, euclidean distance etc. In each iteration, means all of the observations is calculated and then centroid is re calculated until the centroid becomes stable. The mean values of randomly selected centers converge to the appropriate cluster.

The reason to choose this technique is its simplicity and superior performance over its peer methods with reasonable accuracy. However choosing the initial seed is tricky and difficult for achieving best results with high precision.
After obtaining the multi-way association rules, we applied the hierarchical clustering technique. This technique is infact an extended version of K-Means. The end product of this technique resulted in four hierarchical clusters. Among various similarity measures, we chose Euclidean distance whereas the clustering method is average group linkage. Fig 7 shows the dendogram of these hierarchical clusters.

The clustering analysis is used in this paper is K-Means clustering because of its speed and reasonable accuracy. It is however difficult to estimate the k value for each new dataset as well as to maintain high accuracy and precision given the chosen k value. It is due to the fact that the resulting K-Means clusters are partitioned by mean values iteratively. The mean values of randomly selected centers converge to the appropriate cluster. After obtaining the multi-way association rules, we apply the hierarchical clustering technique (which is an extended version of K-Means) on these rules and obtained the four hierarchical

clusters. Similarity measure applied was Euclidean distance and clustering method is average group linkage. Fig 7 shows the dendogram of these heretical clusters.

Heretical clustering produces strong packet type clusters in the data. The Apriori based association rule classifier finds tronger association between flow parameters. The rules with high lift and confidence values represent strong relation to the application. Hence, the rules set help us derive behavior pattern for a particular packet type by looking at their cause-and-effect relations or casual relations. We trace back the flows to the main trace file and we observe a strong probability that those flows belong to a particular type of packet class.

Cluster 1: This cluster shows the transitions which have the multicast addresses.

Cluster1 also contains the three sub-clusters.

Cluster 2: This cluster contains the CBR traffic. CBR traffic is also a multicast traffic. This is one-to-many correspondence between number of senders and receivers

Cluster 3: This cluster shows the TCP type of traffic with acknowledge information.

Cluster 4: This cluster shows the RTP transitions. These transactions also contain the multicast addresses.

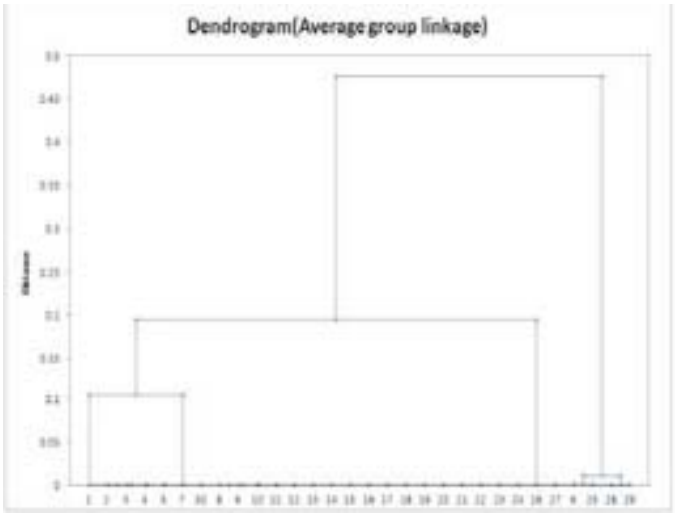

Figure 7. Dendogram of Four Clusters

5. Conclusion

In this paper, we presented the analysis of computer network traffic behavioral pattern for the Transport layer of TCP/IP protocol stack, using unsupervised association rule mining and clustering techniques. K-Means clustering with association rule mining techniques were shown to achieve high accuracy. We have show that our model is able to detect new behavior patterns for multicast traffic. For the future work, we are planning to extend this model to be scalable for a very large trace of dataset which are normally generated in the complex scenario based simulation experiment while soliciting behavior patterns for a wider range of network traffic.

References

[1] Umang, K., Chaudhary, Papapanagiotou, Ioannis., Devetsikiotis, Michael (2010). Flow Classification Using Clustering and Association Rule Mining.

[2] Jeffrey Erman, Martin Arlitt, Anirban Mahanti (2006). Traffic Classification Using Clustering Algorithms, MineNet '06 Proceedings of the 2006 SIGCOMM workshop on Mining network data.

[3] Yu Guan, Ali, A., Ghorbani Nabil Belacel, (2003). Y-MEANS: A Clustering Method for Intrusion Detection, Electrical and Computer Engineering. IEEE CCECE. Canadian Conference, p.1083 – 1086, V.2.

[4] Animesh Patcha, Jung-Min Park, (2007). An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends, Computer Networks.

[5] Smaha, S,E., Haystack (1998). An Intrusion Detection System, *In*: Proceedings of the IEEE Fourth Aerospace Computer Security Applications Conference, Orlando, FL, p. 37–44.

[6] Anderson, D., Frivold, T., Tamaru, A., (1994). A. Valdes, Next Generation Intrusion Detection Expert System (NIDES), Software Users Manual, Beta-Update release, Computer Science Laboratory, SRI International, Menlo Park, CA, USA, Technical Report SRI-CSL-95-0.

[7] Staniford, S., Hoagland,J,A., McAlerney, J,M.(2002). Practical Automated Detection of Stealthy Portscans, *Journal of Computer Security*, 10, p. 105–136.

[8] Ye, N., Emran, S,M.,Chen, Q.,Vilbert, S., (2002). Multivariate Statistical Analysis of Audit Trails For Host-Based Intrusion Detection, IEEE Transactions on Computers. 51, p. 810–820.

[9] Ertoz, L., Eilertson, E., Lazarevic, A., Tan, P, N., Kumar, V.,Srivastava, J., Dokas, P. (2004). The MINDS - Minnesota Intrusion Detection System, in: Next Generation Data Mining, MIT Press, Boston.

[10] Barbara, D., J. Couto, S. Jajodia,Wu (2001). ADAM: a Testbed for Exploring the Use of Data Mining in Intrusion Detection," ACM SIGMOD Record: SPECIAL ISSUE: Special section on data mining for intrusion detection and threat analysis. V. 30, 15–24.

[11] Dickerson, J.E., Dickerson, J.A. (2000). Fuzzy Network Profiling for Intrusion Detection, *In:* Proceedings of the 19th International Conference of the North American Fuzzy Information Processing Society (NAFIPS), Atlanta, GA, p. 301–306.

[12] Mahoney, M.V., Chan,P.K.(2001). PHAD Packet Header Anomaly Detection for Identifying Hostile Network Traffic, Department of Computer Sciences, Florida Institute of Technology, Melbourne, FL, USA, Technical Report CS-4.

[13] Mahoney, M.V., Chan, P.K.(2002). Learning Non Stationary Models of Normal Network Traffic for Detecting Novel Attacks, *In:* Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Edmonton, Canada, p. 376–385.

[14] Valdes, A., Skinner, K. (2000). Adaptive Model-Based Monitoring for Cyber Attack Detection, *In:* Recent Advances in Intrusion Detection Toulouse, France, p. 80–92.

[15] Yu Liu, Yang Li., Hong Man, (2007). A Hybrid Data Mining Anomaly Detection Technique in Ad Hoc Networks, *Int. J. Wireless and Mobile Computing*, 2 (1).

[16] Lee,W., Stolfo, S.J., (1998)"Data Mining Approaches for Intrusion Detection, *In:* Proceedings of the 7th USENIX Security Symposium (SECURITY-98), Berkeley, CA, USA, p. 79–94,.

[17] Ramadas, M.,Tjaden, S,O,B. Detecting Anomalous Network Traffic with Self-Organizing Maps, *In:* Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, USA, p. 36–54.

[18] Xuan Dau Hoang, Jiankun Hu and Peter Bertok, (2003). A Multi-layer Model for Anomaly Intrusion Detection Using Program Sequences of System Calls," Networks, ICON2003, The 11th IEEE International Conference, p. 531–536.

[19] Bouras, C., Gkamas, A., Kioumourtzis, G. (2008). Adaptive Smooth Multicast Protocol for Multimedia Data Transmission, 2008 International Symposium on Performance Evaluation of Computer and Telecommunication Systems – SPECTS, Edinburgh, UK, p. 16–18.

[20] Padhye et al., (1999). A model based TCP - friendly rate control protocol, Proc. International Workshop on Network.

[21] Legout, A., Biersack, E.W. (2000).PLM: Fast Convergence for Cumulative Layered Multicast Transmission, *In:* Proceedings of ACM SIGMETRICS, p. 13-22.

[22] Borgelt, C., Kruse, R., (2002). Induction of association rules: Apriori implementation. In Compstat: Proceedings in Computational Statistics: 15th Symposium Held in Berlin,Germany, p. 395. Physica Verlag,.