A Real Time Intrusion Aggregation And Prevention Technique

Fouzia Sultana
Research Scholar , Department of Computer Science JNTU Hyderabad , Hyderabad
Email: fouzia2005@rediffmail.com
Dr. Stephens Charles
Principal Stanley Stephen College of Engineering Kurnool
Email: stephen@jamindia.com
Dr. A. Govardhan
Director Evaluation and Prof. Dept. of Computer Science , JNTU Hyderabad -72
Email: govardhan_cse@yahoo.co.in

ABSTRACT

Alert aggregation is an important subtask of intrusion detection. The goal is to identify and to cluster different alerts produced by low-level intrusion detection systems, firewalls, etc. belonging to a specific attack instance which has been initiated by an attacker at a certain point in time. Thus, meta-alerts can be generated for the clusters that contain all the relevant information whereas the amount of data (i.e., alerts) can be reduced substantially. Meta-alerts may then be the basis for reporting to security experts or for communication within a distributed intrusion detection system. We propose a novel technique for online alert aggregation which is based on a dynamic, probabilistic model of the current attack situation. Basically, it can be regarded as a data stream version of a maximum likelihood approach for the estimation of the model parameters. With three benchmark data sets, we demonstrate that it is possible to achieve reduction rates of up to 99.96 percent while the number of missing meta-alerts is extremely low. In addition, meta-alerts are generated with a delay of typically only a few seconds after observing the first alert belonging to a new attack instance. Two types of intrusions are detected in this work: Firstly a spam attack is detected based on the blacklisted IP addresses from Stop Forum Spam and secondly packet level intrusion is detected based on KDDcup data. A packet sniffer is designed which keeps sniffing and extracting all the packets that are exchanged over internet interface. The packets are filtered and the headers are extracted. The headers are further subdivided into TCP, IP and UDP headers. ICMP packets are then separated. The data is matched with the database intrusion entries using fast string matching techniques and possible attack entries are marked with different color codes. An attack signature may be visible in any header of the same packet. In such cases, the alerts are aggregated and a single alert is generated. A signature can be mutated to multiple packets with similar signature. Such alerts are also combined to a single alert such that the amount of alert being generated is controlled and that only the signature of the attack is available with the attacker. Results shows that, adaptation of this technique can not only detect all the signatures with .02% false acceptance rate and .06% false rejection rate but at the same time can keep the total number of alerts down below 25% of the overall alerts being generated.

Keywords –**Alert aggregation, attacks, meta-alerts, packets, intrusion detection.**

Date of Submission: 18, December 2013 Date of Acceptance: 14, February 2013

I. INTRODUCTION

The objective of the system is to develop an alert aggregation system for reducing the number of intrusion or other anomaly attacks in a fast string matching based intrusion detection system. Multiple alert of the same signature leads to misleading inferences for intrusion database. Therefore system should be able to detect and store only those intrusions that are relevant for future detection and those that are significantly independent signature. Generally such a system work offline where firstly all the intrusions are marked as they appear and then the aggregation system aggregates the data. But offline aggregation introduces higher latency in detection and reduces the efficiency of the system. Hence we model an online aggregation system for alerts that not only enable fast detection but also aggregates the alerts based on their type over all the detected and incoming packets.

Alert classification and aggregation is of equal importance as that of intrusion detection. Detected patterns or signatures are used for future database for such a system. Intrusion detection systems are generally fast pattern or string matching algorithms that detect the intrusion. Hence a huge database size leads to significant delay in detection. Therefore detected signatures must be aggregated and sorted for precise interpretation of the detection. The work statement can be summarized as to detect packet level intrusion and summarize them for faster interpretation of the intrusion patterns and for future reuse of the patterns.

The work can be used in following applications:

- For detecting online packet level anomalies and intrusions.
- For segregating the anomalies based on the type of packet or field. For example a port based anomaly must be used as a different entity than a ttl based anomaly.
- For keeping the number of alerts low in order to derive inferences from the alerts
- To derive meaningful session intrusion patterns that reveal the order or group of intrusion for particular group of access data.
- Can be used as a secondary firewall to filter the packets that match with the past true positive signatures.

II. PROPOSED WORK

2.1 Existing System

- Most existing IDS are optimized to detect attacks with high accuracy. However, they still have various disadvantages that have been outlined in a number of publications and lot of work has been done to analyze IDS in order to direct future research.
- Besides others, one drawback is the large amount of alerts produced.
- Alerts can be given only in System logs.
- Existing IDS does not have general framework which cannot be customized by adding domain specific knowledge as per the specific requirements of the users or network administrators.

In short while an intrusion is detected through any of the technique, the administrator will be more interested to know the type of attack for example a smurf, a Perl attack and so on, rather than which port causes the attack.
Various ports and IP address may lead to same type of attack. Hence attack classification should be one of the major entities of an intrusion detection system. In general the current system adopts offline classification of the alerts where the alerts are first logged as they come and then they are classified based on learning rule.

III. RELATED WORK

[1] In this paper the authors define Intrusion Detection System as an emerging technology for detecting the unauthorized users and malicious behavior in a system. Alert supervision is proved to be tedious in intrusion system, so Meta-alerts are proposed. Meta-alerts are simple alert patterns that can identify any pattern in the network.

The primary objective is to generate meta-alerts using probabilistic technique with offline and online alert aggregation using generative modeling is shown in paper [2] by M. Thangavel and P. Thangaraj. The system transforms random attacks into models. To defend against multi-step intrusions in high speed networks, efficient algorithms are needed to correlate isolated alerts into attack scenarios with finite memory, the index can only be built on a limited number of alerts inside a sliding window. Knowing this fact, an attacker can prevent two attack steps from both falling into the sliding window by either passively delaying the second step or actively injecting bogus alerts between the two steps.

In [3] authors first address the above issue with a novel queue graph (QG) approach. Instead of searching all the received alerts for those that prepare for a new alert, we only search for the latest alert of each type.

Intrusion actions caused by a single attack instance of particular type, often results in hundreds or even thousands of alerts instead of single alert. This makes ambiguity to network security engineer. The primary goal of this work is to identify and to cluster different alerts belonging to a specific attack instance with the concept of alert aggregation. The concept is adapted from the approach presented in [4].

Traffic anomalies and distributed attacks are commonplace in today's networks. Single point detection is often insufficient to determine the causes, patterns and prevalence of such events. Most existing distributed intrusion detection systems (DIDS) rely on centralized fusion, or distributed fusion with unscalable communication mechanisms

Paper [5] presents a design of an operational model for minimization of false positive alarms, including recurring alarms by security administrator.

In [6] cluster based anomaly detection is done instead of considering individual alerts forms a cluster depending upon similarities in the behavior. Therefore further alerts are easily classified and clustered.
Comprehensive Approach to Intrusion Detection Alert Correlation is demonstrated in [7] which is a general correlation model that includes a comprehensive set of components and a framework based on this model. A tool using the framework has been applied to a number of well-known intrusion detection data sets to identify how each component contributes to the overall goals of correlation. Firstly like any other IDs, we develop and setup a

detection database that provides the rules for detections. Packets are captured in real time over the network interface and are compared with the database. As the packets are fragmented into subcategories, any possible attack may meet similarity with multiple detection patterns. Hence rather than marking them separately, the system aggregates them based on the closeness with a database entity and already detected entity Online Intrusion Alert Aggregation with Generative Data Stream modeling is a generative modeling approach using probabilistic methods. Assuming the attack instances as random process producing alerts ,we aim at modeling these processes using approximate maximum likelihood parameter estimation technique. Thus, the beginning as well as the completion of attack instances can be detected .

In the proposed scheme of Online Intrusion Alert Aggregation with Generative Data Stream modeling we extend our idea of sending Intrusion alerts to the mobile, this makes more comfortable.

[8] Proposes secure multiparty computation (MPC), which allows joint privacy-preserving computations on data of multiple parties. This is important framework as it defines the event driven correlation in the computation environment.

The authors in [9] emphasizes on Alert correlation, which is a crucial problem for monitoring and securing computer networks.

In [10] authors propose to build a DIDS based on the emerging decentralized location and routing infrastructure: *distributed hash table (DHT).*

Fredrick Valeurs in paper [11] claims that producing a high number of alerts does not mean that the attack detection rate is high. In order to increase the detection rate, the use of multiple IDSs based on heterogeneous detection techniques is a solution but in return it increases the number of alerts to process. Aggregating the alerts coming from multiple heterogeneous IDSs and fusing them is a necessary step before processing the content and the meaning of the alerts.

[12] Is the complete thesis work of Fredrick on Real-Time Intrusion Detection Alert Correlation.

Online Intrusion with Generative Data Stream Modelling does not degrade system performance as individual layers are independent and are trained with only a small number of features, thereby, resulting in an efficient.

Online Intrusion Alert Aggregation with Generative Data Stream Modeling is easily customizable and the number of layers can be adjusted depending upon the requirements of the target network. Our framework is not restrictive in using a single method to detect attacks. Different methods can be seamlessly integrated in our framework to build effective intrusion detectors.

Our framework has the advantage that the type of attack can be inferred directly from the layer at which it is detected. As a result, specific intrusion response mechanisms can be activated for different attacks.

IV. METHODOLOGY

4.1 Misuse and Anomaly Detection ALGORITHM*:*

Step 1: Select the ‘n’ layers needed for the whole IDS.
Step 2: Build Sensor Layer to detect Network and Host Systems.
Step 3: Build Detection Layer based on Misuse and Anomaly detection technique.
Step 4: Classify various types of alerts. (For example alert for System level intrusion or process level intrusion)
Step 5: Code the system for detecting various types of attacks and alerts for respective attacks.
Step 6: Integrate the system with Mobile device to get alerts from the proposed IDS.
Step 7: Specify each type of alert on which category it falls, so that user can easily recognize the attack type.
Step 8: Build Reaction layer with various options so that administrator/user can have various options to select or react on any type of intrusion.
Step 9: Test the system using Attack Simulation module, by sending different attacks to the proposed IDS.
Step 10: Build a log file, so that the reports can be saved for future work.

4.2 Color Scheme

```
 Intrusion
========================
If Src found in database =Orange
If Dst found in database=Maroon
====================

 ======IP===============
TTl>110=Red
TotalLength<20 || TotalLength>1200=Cyan
DiffSerrice!=0x00=Blue
======================


========TCP===============
Port!80=RED
Window<10000=Bisquit color
DestinatioPort>40,000=Violet
========================
```

TCP
UDP
Unknown

Fig. 1 Class Diagram of Work

4.3 Results

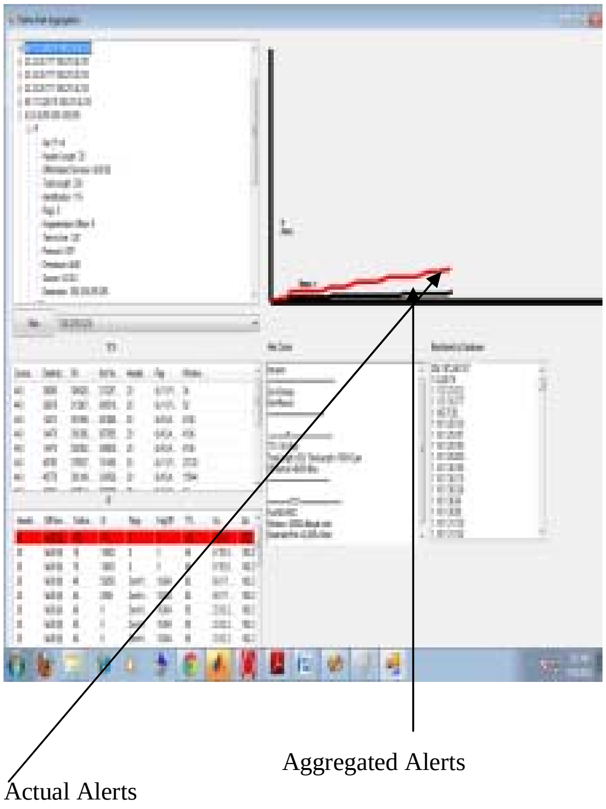

Fig 1 Online Alert Aggregation

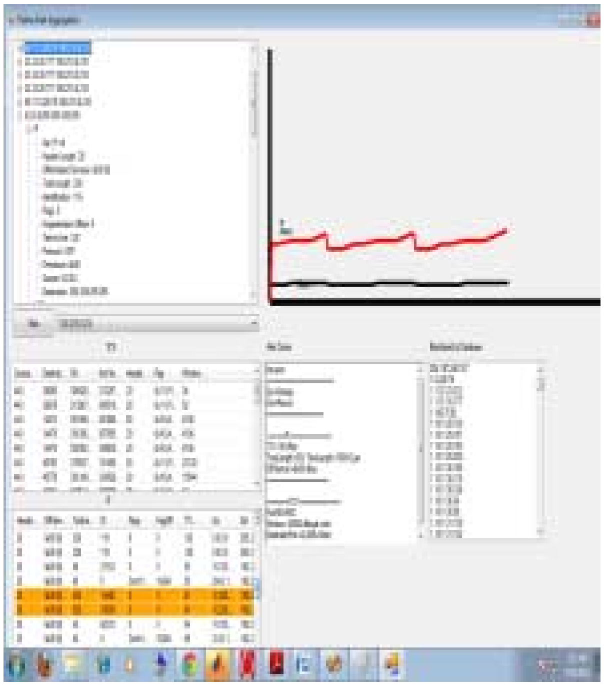

Fig 2. Multiple Alerts

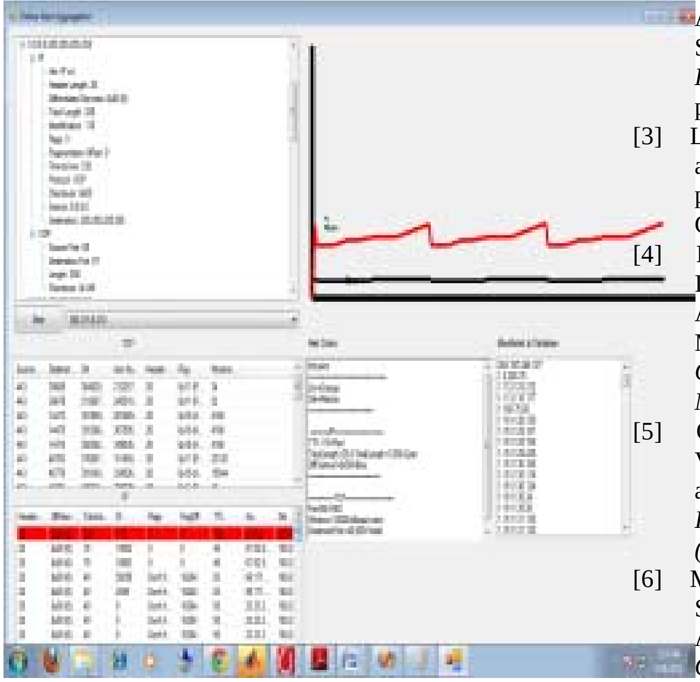

Fig 3. Fragmentation of Packets

V. Conclusion

The experiments demonstrated the broad applicability of the proposed online alert aggregation approach. We analyzed three different data sets and showed that machine-learning-based detectors, conventional signature based detectors, and even firewalls can be used as alert generators. In all cases, the amount of data could be reduced substantially. Although there are situations specially clusters that are wrongly split—the instance detection rate is very high: None or only very few attack instances were missed. Runtime and component creation delay are well suited for an online application.

The system can be improved further by incorporating learning based aggregation where the learning rule can be set from predefined database in SVM based machine or other kernel technique.

References

Journal Papers:

[1] Adelina Josephine D , Anushiadevi R, Lakshminarayanan T R,” An Efficient Algorithm For Clustering Intrusion Alert”, *Journal of Theoretical and Applied Information Technology. Vol. 37 No.2* ISSN: 1992-8645, March 2012 pp234-240.

[2] M. Thangavel, P. Thangaraj,” Data Stream Intrusion Alert Aggregation for Distributed Heterogeneous Sources”, *European Journal of Scientific Research,ISSN 1450-216X Vol.54 No.3* (2011), pp.375-383.

[3] Lingyu Wang , Anyi Liu, Sushil Jajodia,” Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts”, Computer Communications 29 (2006) pp2917–2933

[4] E.Anitha. C.Swarnambigai .” A Novel Online Intrusion Detection System Based On Alert Aggregation With Data Stream And Generative Modeling”, *International Journal Of Communications and Engineering Volume 05– No.5*, Issue: 01 March 2012.

[5] G. Jacob Victor, Dr. M Sreenivasa Rao, Dr. V. CH. Venkaiah,” Intrusion Detection Systems - Analysis and Containment of False Positives Alerts”, *International Journal of Computer Applications (0975 – 8887) Volume 5– No.8,* August 2010.

[6] M. Thangavel, P. Thangaraj, “ Cluster based Statistical Anomaly Intrusion Detection for Varied Attack Intensities”, *International Journal of Computer Applications (0975 – 8887) Volume 24– No.9,* June 2012.

[7] Fredrik Valeur, Giovanni Vigna, Member, IEEE, Christopher Kruegel, Member, IEEE, and Richard A.. Kemmerer, Fellow, IEEE,” A Comprehensive Approach to Intrusion Detection Alert Correlation”, *IEEE Transactions On Dependable And Secure Computing, Vol. 1, No. 3,* July-September 2004.

[8] Martin Burkhart, Mario Strasser, Dilip Many, Xenofontas Dimitropoulos, "SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics",

[9] Karim Tabia1, Salem Benferhat1, Philippe Leray2, Ludovic M´e3, "Alert correlation in intrusion detection: Combining AI-based approaches for exploiting security operators' knowledge and preferences " ,Copyright c 2011, Association for the Advancement of Artificial

[10] Zhichun Li, Yan Chen, Aaron Beach,"Towards Scalable and Robust Distributed Intrusion Alert Fusion with Good Load Balancing", *SIGCOMM'06 Workshops* September 11-15, 2006, Pisa, Italy. Copyright 2006 ACM 1-59593-417-0/06/0009.

[11] Fabien Autrel et Fr´ed´eric Cuppens, " *Using an Intrusion Detection Alert Similarity Operator to Aggregate and Fuse Alerts*", GET-ENST-Bretagne, 35576 Cesson S´evign´e (France).

[12] Fredrick Valeur , *Real-Time Intrusion Detection Alert Correlation*, doctoral diss., University of California, Santa Barbara May 2006.

Authors Biography

Mrs. Fouzia Sultana is a research scholar in Computer Science faculty, pursuing Ph.D from JNTU Hyderabad in area of Network Security .She has completed her B.E in Computer Science and Engineering in the year 1989 from PDA College of Engineering, Gulbarga and M.E in Computer Science and Engineering in 1999 from KBN College of Engineering, Gulbarga affiliated to Gulbarga University, Gulbarga. She started the career as a lecturer at KBN College of Engg. in 1990 later then served same Institute as Asst. Professor and Head of the CSE Dept from 1999-2008.Worked as a Professor at Aurora's Engg. Colleges, Bhongir Hyderabad from 2008-2010.Her area of interests are Networking Network and Web Security. She was earlier a member College Academic committee at AEC. Bhongir and a Life member of **ISTE.**

Dr. Stephen Charles received ME degree from Bharathiar University, Coimbatore and PhD from Jawaharlal Nehru Technological University Hyderabad. He is working as a Principal in Stanley Stephen College of Engineering, Kurnool. He has 23 years of experience in teaching His research interests are digital signal processing, Network Security Information Security and Wireless networks. He published 18 International journal Papers and 2 National Journal papers, 35 International conference papers. He has guided 3 candidates for their Ph.D.

Dr. A Govardhan did his Intermediate from APRJC Nagarjuna Sagar, during 1986-1988, BE in Computer Science and Engineering from Osmania University College of Engineering, Hyderabad in 1992, M.Tech from Jawaharlal Nehru University(JNU), Delhi in 1994 and he earned his Ph.D from Jawaharlal Nehru Technological Univesity, Hyderabad in 2003.He is the Director Evaluation JNTU Hyderabad. He guided 10 Ph.D theses, 1 M.Phil and 123 M.Tech projects. He has 152 Research Publications in International/National Journals and Conferences. Dr. Govardhan is a Member in Executive Council, JNTUH, He is a member of Standing Committee for Academic Senate, JNT University Hyderabad and Academic Advisory Committee (**AAC),** UGC-Academic Staff College and Sports Council, JNT University Hyderabad. He is a Member on the Editorial Boards for Seven International Journals. He had attended an International Conference in Stockholm, Sweden. He is also a member in various Professional and Service-oriented bodies. He had received the best teacher award from Andhra Pradesh Govt. in the year 2011-12. This year he has been a selected for a prestigious "Dr Sarvepally Radhakrishna" NATIONAL Award.