ALERT CLUSTERING METHOD FOR INTRUSION DETECTION

J.Jegan Amarnath\textsuperscript{1} *, Pradeep Kumar Sahoo\textsuperscript{2}, J.K.Periasamy\textsuperscript{3}, Sanjana. D\textsuperscript{4}

\textsuperscript{1,2,3,4}Department of Computer Science and Engineering, Sri Sairam Engineering College, Chennai, India.
\textsuperscript{1} jegan.cse@sairam.edu.in, \textsuperscript{2} pradeep.cse@sairam.edu.in, \textsuperscript{3} jkperiasamy@gmail.com

February 12, 2018

Abstract

The main objective of the project is to overcome the major challenging problem for cloud providers. So Planning to design efficient mechanisms related to storage allocation for storing a data and binary content like video and audios. The new mechanisms are available for the cloud providers to effectively utilize the resources with minimum cost and maximum profit. To overcome the failure and maintain the integrity and recovery of the data, Cloud providers have introduced server based models for VM provisioning and allocation which allow the users to recover the datas from the redundant copy of the disk sharing over the server from VMs. API acts as interface to upload the jar files. Here the VMs physical storage is equally fragmented. All the files get replicated by its default. There is a less chance of data has been lost in the server even though there is failure in the system component in server side that data might be stored in the virtual storage. Any one of the file server get failure the master copy will be send to other files server then they equally shared again the original data will replicated to other remaining server. Then the original files get cluster
together. In this project, the dynamic VM provisioning the formulate and allocation problem for the failure of resources. Project have design the data split and join mechanisms for the problem such that the cloud provider provisions VMs based on the requests of the users. This project performs extensive experiments using real workload traces in order to deal the performance of the proposed mechanisms.

**Key Words:** VM (virtual machine), API (application programming interface), Cloud Providers, Clustering, Intrusion Detection.

1 INTRODUCTION

With the fast evolvement of mobile Internet, people are concentrating more on the wireless network security problem. But due to the complexity of the wireless network, at present it is difficult to see the exploration of wireless intrusion alerts clustering method for mobile Internet. This paper propounds a Wireless Intrusion Alert Clustering Method (WIACM) based on the information of the mobile terminal. The method includes alert formatting, alert reduction and alert classification. By propounding main information of the mobile terminal device, this method accumulates the original alerts into hyper alerts. The earlier results show that WIACM would be proper for real attack scenarios of mobile Internet, and reduce the amount of alerts with more accuracy of alert analysis.

Smart Phones laptops, tablets, laptops and other portable computing devices are protected by mobile network security also knows as wireless security and they connected networks to/from threats and vulnerabilities associated with wireless computing.

Securing mobile devices has become increasingly important in recent years as the numbers of the devices in operation and the uses to which they are put have expanded dramatically. The complex problem is connected within the enterprise in the recent IT trends and consumerization is resulting in more and more employee-owned devices connecting to the corporate network.

Mobile Internet security becomes one big issue in the network security field. There are two types to prevent the system, one is intrusion detection and another one is intrusion prevention[1].
2 RELATED WORK

[1] In “A survey of intrusion detection and prevention systems”, Patel Ahmed, Qassim Qais, Wills Christopher have analysed the large and growing area of concern for every network which is the network security. Most of the network environments keep on facing an ever increasing number of security threats in the form of Trojan worm attacks and viruses that can damage the computer system and communication channels. Firewalls are used as a security check point in a network environment but still different types of security issues keep on arising. In order to further strengthen the network from illegal access the concept of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) is gaining popularity.

[2] In “Intrusion detection for wireless mesh networks using finite state machine”, Yi Ping, Wu Yue, Liu Ning, Wang Zhiyang, have analysed an adaptive on-line algorithm to detect such selfish behavior based solely on local observations of messages exchanged by AODV-like routing protocols. We use a finite state machine model of locally observable protocol actions to generate a statistical description of the behavior of each neighbor and apply statistical analysis to cluster neighboring nodes on the basis of behavioral similarities and identify the selfish ones.

[3] In “A survey of intrusion-detection alert aggregation and correlation techniques”, Mu Chengpo, Huang Houkuan, Tian Shengfeng have proposed a method to overcome the difficulty in the field of intrusion detection and that is the organization of alerts. Normally IDSs produced number of alerts. But the analyst could not understand what type of alert occur and which type of alert is generated etc. because of the huge number of alerts generated by these systems. One solution of this problem is classifying the alerts. During this paper, we try to represent an overview of IDS alerts classification techniques.

3 PROPOSED SYSTEM

The WIACM method contains three steps which are called the alert formatting, alert reduction, alert classification which lends the result which is that the alerts are well organised and it is easier for
the server to distinguish the alerts and act accordingly. The classification in the end helps us with to classify the type of alerts and help the server in the future.

**Advantages:**

1. The three steps of filtering the alerts in parallel results in time efficiency.

2. The reduction part helps to cut out the unrelated alerts. For example WEP crack alerts generated on an AP while its encryption.

3. It helps in reducing the repetitive alerts leading to less alerts which in turn prevents bottlenecks.

Fig.1 Architecture Diagram
3.1 METHODOLOGY

3.2 NODE CONFIGURATION

Wireless nodes are created in the wireless network scenario that has been decided in the plant manner. Node configuration essentially consists of defining the different node characteristics before creating them. They may consist of the type of addressing structure used in the simulation, defining the network components for mobile nodes, turning on or off the trace options at Agent/Router/MAC levels, selecting the type of ad-hoc routing protocol for wireless nodes or defining their energy model. Simulator::node-config accommodates flexible and modular construction of different node definitions within the same base Node class. For example, Wireless communications have capable of creating new wireless nodes, one no longer needs a specialized node creation command.

![Node Configuration](image)

NODE CONFIGURATIONS ified as safe which is not possible unless he already has access to users email account. Fig. 2. Node Configuration

3.3 FORMATTING OF ALERT

First step is security alerts captured by IDS installed in the wireless sensors, and improving their IDMEF alert format, in which we
introduce information about AP, mobile terminals and its types, and the SSID, working channel, the MAC address, signal strength, whether encrypted or not and encryption mechanism of the AP, which reflect the characteristics of the mobile Internet environment.

3.4 REDUCTION OF ALERT

Alerts produced by wireless intrusion detection system contain a large number of repetitive and unrelated alerts, such as alerts generated for WEP crack on an access point (AP) while its encryption scheme is WPA, repetitive alerts for the same continuous attacks and so on. Therefore it is necessary to eliminate and reduce the alerts to improve the accuracy and reliability of the analysis of the alerts.
3.5 CLASSIFICATION OF ALERT

For the reduced alerts, they introduce the SSID of AP and MAC address of the attack source and target to classify alerts into hyper alerts, which belongs to one kind of attack security alerts with obvious attack behavior characteristics and improves the accuracy of intrusion detection.

3.6 PERFORMANCE EVALUATION

During simulation time the events are traced by using the trace files. The performance of the network is evaluated by executing the trace files. The events are recorded into trace files while executing record procedure. In this procedure, we trace the events like packet received, Packets lost, Last packet received time etc. These trace values are write into the trace files. This procedure is recursively called for every 0.05 ms. so, trace values recorded for every 0.05 ms.

Fig.5. Performance Evaluation
4 FUTURE WORK

The future enhancement will be of the prevention of sink hole attack where the attacker can drain out the energy out of the other node and can cause a significant damage to the user.

References


