Providing Network Security using Intrusion Detection System with Generating Meta Alerts

Miss. Borhade S. R.1 Prof. Kahate S. A.2
1 M.E. Student 2 Assistant Professor & Guide & PG Coordinator
1,2 Department of Computer Engineering

Abstract—IT systems are the main component of humans life in which networking is essential thing. When networking is considered the first thing which comes in everyone’s mind is security. To ensure this security mechanisms IDS(Intrusion Detection System) comes into picture. This technology is an important aspect in the process of designing a environment which is secure. The main aim of this technology is to detect suspicious attack and collect or generate the alerts. The IDS which are existing e.g. firewalls, snort creates large number of alerts. Due to large number of alerts there are many chances of system admin getting confused that which action should be performed on which attack. This results into delay in decision making. This paper aims to meta-alert generation by aggregating alerts. Meta-alerts can be easily understood by system admin/network administrator and supportive action can be easily performed. Generative Data stream modeling approach can be used to generate meta-alerts.

Key words: IDS Intrusion Detection System, Generative Data Stream Modeling, Meta-Alert Generation, Alert Aggregation

I. INTRODUCTION
Today's world is IT world. In Information Technology Data is essential thing. Sharing of data is done through networking. In networking security is most important aspect for secure environment. To create this secure environment, the technology which comes into mind is Intrusion Detection System (IDS).

IDS play a very important role in creating environment which is secure. As the network increases, the relevant technologies also increase. At the same time various kinds of threats are also increases. These threats are known as attacks. These attacks can be prevented by using following techniques like authentication, authorization, integrity, encryption and decryption. At the same time along with the above techniques Virtual Private Network can be used.

The most recent technique to create secure environment is IDS (Intrusion Detection System). Existing IDS such as firewalls, snort are not efficient. This Intrusion Detection Systems are capable of detecting intrusions at the time when intruder tries to intrude into the network.

This system of intrusion detection can work in two ways i.e. independently or in a distributed environment. It can be used in multiple type of network such as wireless sensor networks and mobile Ad Hoc networks and many more. There are mainly two types of IDS. They are known as host based and network based. They are used to detection of anomaly detection of misuse or detection of intrusion[2]. The IDSs are very necessary for the security requirement. The networks which use protocols like transmission control protocol and user datagram protocol can be monitor through short. It can prevent attacks like SQL Injection, buffer overflow, denial of service and many more.

This IDSs detects the attacks and generates the alerts. The alerts are generated in multiple numbers. Due to large number of alerts generated, network administrator may get confused about actions. This may leads into wrong decision also for this reason it is mandatory to generate meta alerts which is more helpful.

The main purpose of this paper is to collect the flood of alerts and produce meta alerts to instruct network administrator about actions.

This aggregation is achieved by using instances of alerts and grouping them by considering some parameters. The following approach used in this papers are
- Probabilistic methods based on generative modeling
- Data streaming approach for online intrusion alert aggregation

II. RELATED WORK
Intrusion detection system is a mechanism which provides protection in IT services. Many researchers have found that IDSs present in the real world now are effective any provides right decision. But some researchers found problems in producing flood of alerts. There are several approaches came into IDS with respect to alert correlation.

In [2] ultimate solution is created for alert correlation. Instances of attack recognition are a technology used. Alert duplication problems are explored in [3], Where a solution is explained co aggregate the alerts to provide proper message to network administrator. In [4] alert clustering is used to group similar attack instances. In [5] alert correlation is based on weighted attributes. This approach proposed in [6] & [7] suffer from multiple disadvantages like parameters same happened with [8]. In [9] proposed is user has to give parameters same problem happened with [10]. Grouping is based on IP is proposed in [11] & [12]. Many similar techniques were presented in [13],[14] & [15]. In [16] author Kothawale Ganesh in his paper "Online Instruction Alert Aggregation with Generative Data stream Modeling” proposed a somewhat similar approach used in this paper, it focuses on meta-alert generation. This works on both online and offline scenarios. Our approach is presented in the next section.

III. ONLINE ALERT AGGREGATION TECHNIQUE
In this paper we present alert aggregation technique based on probabilistic model. The main goal of this new approach is to effective aggregation of alerts and generating meta-alerts which will help network administrator to take a faster or quick decision. The approach we are proposing in this paper is as follows:
Providing Network Security using Intrusion Detection System with Generating Meta Alerts

As seen in fig(1), the proposed system consists of multiple layers i.e. Sensor layer, Alert processing Layer, Reaction layer.

Sensor layer creates TLP and UDP traffic. It monitors this traffic. Detection of intrusion base on anomaly or misuse detection is done in detection layer one more important task is to generate alerts and send it to alert processing layer. The main aim of alert processing layer is to generate alerts based on probability theory. At last reaction layer collects aggregated alerts and generates meaningful action reports to system administrator.

IV. OFFLINE ALERT AGGREGATION

The algorithm for offline alert aggregation will be extended to a data stream algorithm for online aggregation. We suppose that TCP and UDP traffic is attacked by attacker all the alerts are marked with false negative and false positive. The above information is logged and can be used to aggregate the alerts offline. Following are some challenges in alert aggregation.

- Inability to recognize false alerts.
- Placing of false alerts in incorrect cluster.
- Wrong aggregation of alerts.
- Wrong grouping of alerts.

The algorithms for alert aggregation which works offline is described in fig(2).

V. OFFLINE ALERT AGGREGATION ALGORITHM

From above fig(2) it clearly seen that there are some steps which comes after the algorithm such as initialization of parameters alerts to components assignment, stopping criteria checking coefficients working.

In initialization we obtain accurate initial values. After this process the generates alerts are added to specific components. Next process is of checking condition for stopping process. At last for optimization coefficient helps.

VI. DATA STREAM ALERT AGGREGATION

The above algorithm shown in fig (2) is developed further to generate online alert aggregation. It requires following steps to follow:

1) Adaptation of component
2) creation of component
3) detection of component

The above all the steps are self-explanatory. Final step is meant for component detection and it helps in aggregation of alerts.

The algorithm for data stream alert aggregation is described in fig (3) creation of component is done as shown in following algorithm:
Algorithm 3: Component Creation in Case of Detected Novelty Input: partition C, specific cluster number j*, Buffer B Output: updated partition C
1) \( C' := C \setminus C_j^* \)
2) For k=1 to K do
3) \( C(k) := ALG1(C_j^* \cup B, K) \)
4) \( \Omega(k) := \Omega(C' \cup C(k)) \)
5) \( K^* := \text{argmax } \Omega(k) \text{ } \forall k \in \{1, \ldots, K\} \)
6) \( C := C' \cup C(k^*) \)

VII. IMPLEMENTATION AND RESULTS
The IDS has been developed by java programming languages, Net Beans, JDK and JME. Operating system or OS is Windows XP OS which run in a PC with 1GB RAM and core 2 duo Processor. GUI has been developed with AWT & SWING API of JAVA. UI is build for attack simulation &other interfaces.
Fig 4, 5& 6 shows the UI for Attack simulation and action report.

Fig 4: GUI for attack simulation

Fig 5: GUI for attack simulation

Fig 6: GUI for action Messages Displayed

VIII. CONCLUSION
Thus we can conclude that online intrusion alerts aggregation can be easily done through generative data stream modeling which is depends on probabilistic method. It is found that meta-alerts are produced efficiently. Missing false alerts rate can also be reduced to get higher accuracy. Also IDS accuracy can also been increased. Number of attacks detected is more as compared to alerts produced. Thus Online Intrusion alert aggregation with generative data stream modeling is very efficient and secure in IT services.

REFERENCES