ODS-MAS: New Approach on Obtrusion Detection System using Mobile AgentS Based Data mining.

[1] N.Priyadharshini, [2]R.Ramprashath,
[1] Assistant Professor, [2]Assistant Professor
[1]Department of Computer Science, [2]Department of MCA
[1] Sree Saraswathi Thyagaraja College, [2]Karpagam College of Engineering, Coimbatore, TamilNadu, India.

Abstract : Intrusion Detection has been detected since many years and the area attained the next level. Indeed , the confrontation grow, e.g., how an Intrusion Detection System (IDS) can detect distributed attacks. To gear up with the solution, we propose a dispensed IDS, with available support of mobile agent methodology and the exactness supplied by the data mining skills.

Key Terms— **Intrusion Detection System, Mobile Agents, Filter Agents, Data Mining Techniques.**

I. INTRODUCTION

A doorway of a network, Intrusion Detection Systems (IDS)s have the quality to find and oppose the Obtrusion sharp and fast. How- ever, most current IDSs are centralized and thus a central analyzer presents a favorable target to the attackers [1].

In this paper, we carry out a systematic another way of gearing up this problem. And through the advantages of mobile agent methodology, that has: depletion of network burden, solving network latency, system capacity to be changed in size or scale., etc, this methodology seems effectively solve obtrusion detection in a distributed environment [2]. We gears up with a new dispensed IDS, called ODS-MAS (Obtrusion Detection System using Mobile AgentS based Data mining). The ODS-MAS system, in-turn connects the data mining and the mobile agents in to find informed and uninformed defends.

1.1 THE ODS - MAS SYSTEM

The mobile agent is the code/object on move which travels in its itinerary within the network of connected nodes.[3] The figure 1 depicts the architecture of ODS-MAS.

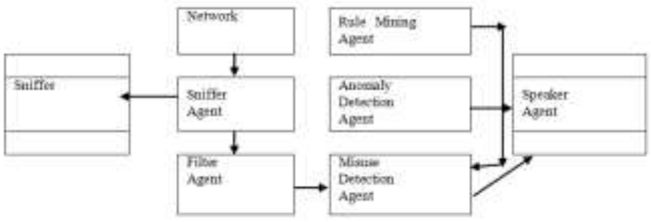


Figure 1: Architecture of ODS-MAS

A dispensed structure is made up of various agents that is capable of taking a start form one place and reaches another station usually: Sniffer, Filter, Misuse Detection, Anomaly Detection, Rule Mining and Speaker Agent [5].

1.2 The Sniffer Agent

A Sniffer is a program on the network traffic by grabbing information travel-ling over a network . Mobile agents figure 2 depicts the method it perform a task by migrating and executing on several nodes connected to the network. Ignored to detect sniffers [4], the network administrator sends some special types of mobile agents in the network and collects information from different nodes.

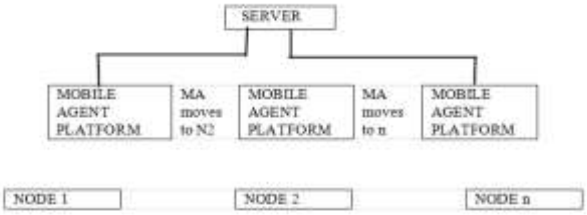


Figure 2 : Migration of the Sniffer Agent

The Sniffer Agent collects the network packets and stores them in a “sniffing file”. The benefits of this kind of agent include: i) the cloning and the distribution throughout the network; and ii) the duplication in order to lighten the network charge.

1.3 The Filter Agent

The Filter Agent aggregates and merges events stored in the sniffing file. It performs its tasks as a pre treatment phase, which precedes the analysis phase, Where each points (xi) can be more than MA in same time, then the degree according to distance between them is center (vj)and the point. To minimize with the time taken with objective function [6]:

$$Jm = \sum_{j=1}^{c} \sum_{i=1}^{n} \mu_y d_y \qquad (1)$$

Where $d_y = ||x_i - v_j\ ||$ (2)

The fuzzy steps

The Algorithm Fuzzy C –Means steps are :

1. Initialize U=[Uij] matrix, U(0).

2. At k–step: calculate the centers vectors C(k)=[cj]with U(k) [6]

$$v_j = \frac{\sum_{i-1}^{n} \mu_{ij}^{m} x_i}{\sum_{i-1}^{n} \mu_{ij}^{m}} \qquad (3)$$

3. Update U(k), U(k+1)

1.4 The Misuse Detection Agent

The function of the Misuse detection agent is to find the informed attacks in networks. It is detected by comparing the signatures of filtered packets and attack signatures. Hence, if there is a similarity between the filtered packets and attacks signatures, then the agent knocks over an alert. In turn, it eliminates the misused known packets for further movements. These agents can find and defense only the known attacks.

1.5 The Anomaly Detection Agent

The Anomaly Detection Agent provides the combination of distributed IDS with clustering techniques. The technique gears up the to find the uninformed attacks without delaying on system performance. The clustering-based anomaly detection algorithm is based on the steps described as follows[1]:

Pace 1 (Initialize) : The working data is partitioned to k clusters;

Pace 2 (Assign) : Prepare to post each in nearby cluster;

Pace 3 (Update) : The mean of data members are updated to respective center;

Pace 4 (Iterate) : Pace 2 and 3 iterated till the updates are available;

Pace 5 (Anomaly Detection) :

For each data test occurrence M:

1. Calculate the Euclidean length between M a beginning cluster Ci;
2. Detect the cluster Ci nearest to M;
3. Arrange M as an anomaly or a normal occurrence with existing Threshold.

1.5 The Rule Mining Agent

The agent throws out the required collection of discovered anomalous connections. The manipulation of complete association rule takes places in our Intelligent server (I-server) which contains an Movable Intelligent Agent (MIA) and few immovable agents(ImA). The dividers made earlier are placed in isolated sites in distributed environment [7].The association rules in mining is incorporated with the Informative Generic Basis (   ) [6]. In turn, removes the repetition and applied during an obtrusion detection process provides: the increment of complete coverage of informed attacks and summarizes the needed knowledge, when the information is lossless [6]. It results in the database of signatures of the Misuse Detection Agent and modified in regular routine by the validation of the extracted rule set.

1.6 The Speaker Agent

The administrator receives the detected results from Misuse and the Anomaly findings through the Speaker Agent.

III EXPERIMENTAL RESULTS

3.1 Algorithm

Level 1: The computation begins from packet 1. e.g the service.

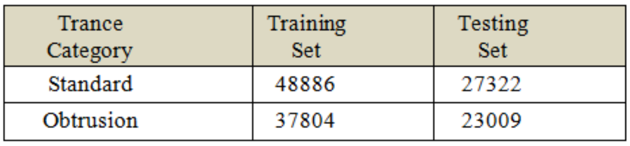
Level 2: The attributes are calculated while the connection is active.

Level 3: The attributes are calculated at the last point of connection and verified.

Level 4: The attributes are calculated at the last, still it needs an active connection.[8]

```
If (H1(X) =Standard) V (H1(X)=Obtrusion) then
        -if H2(X) = Standard
   then
   Output ← H1(X) (Standard or Obtrusion)
   -else
   Output ← New obtrusion
Else
Output ← H1(X)
```

The below Table 1 depicts the results of experiments that had partly used the traffic data DARPA[3]. It shows the dispensed records during the training and testing datasets.



Trance Category	Training Set	Testing Set
Standard	48886	27322
Obtrusion	37804	23009

Table 3.1: Experimental Results

3.2 Metrics

To calculate the working of an ODS, two metrics as:

Metrics 1: The Finding Rate (FR), counts the obtrusion finding number;

Metrics 2: The Fake Constructive Rate (FCR), counts the wrongly found obtrusion number.

The finest piece of anomaly clustering-based algorithm obtained when FR = 89.89% and FCR = 1.00%.

IV Conclusion

In this paper, a dispensed multi-agent ODS architecture, called ODS-MAS was presented. The methodology combines the data mining techniques and mobile agents to contain the essentials in dispensed Distributed Systems. The initial results from experiments shows that mining algorithms used in ODS-MAS will be viable for finding the attacks within a dispensed environment.

V References

1. MAD-IDS: Novel Intrusion Detection System using Mobile Agents and Data Mining Approaches Imen Brahmi1, Sadok Ben Yahia1, and Pascal Poncelet2

2. N. Jaisankar, R. Saravanan, and K. D. Swamy. Intelligent Intrusion Detection System Framework using Mobile Agents. International Journal of Network Security and its Ap- plications (IJNSA), 1(2):72–88, 2009.

3. Singh chowhan, Rahul; purohit, Dr. Rajesh (2016-12-15). "Study of Mobile Agent Server Architectures for Homogeneous and Heterogeneous Distributed Systems". IJCA. 156: 32–37. doi:10.5120/ijca2016912420. Retrieved 2016-12-18.

4. H. M. Kortebi AbdelallahElhadj, H. M. Khelalfa, An experimental sniffer detector: Snifferwall, (2002).

5. S. Ben Yahia, G. Gasmi, and E. Mephu Nguifo. A New Generic Basis of Factual and Implicative Association Rules. Intelligent Data Analysis (IDA) , 13(4):633–656, 2009.

6. Bruno A. Pimentel, Renata M.C.R. de Souza, "A multivariate fuzzy cmeans method", Applied Soft Computing, Elsevier B.V., Vol 13, Issue 4, pp. 1592 – 1607, April 2013.

7. N.Priyadharshini, V.Narayani, “Intelligent Agent For Distributed Environment In Business tactics IADE-BT”, International Journal of Scientific & Engineering Research, Volume 6, Issue 3, March-2015, ISSN 2229-5518

8. Priya U. Kadam1, Prof.Manjusha Deshmukh2, International Journal of Innovative Research in Computer and Communication Engineering, “ Various approaches for Intrusion detection System: An overview”.

9. A.Pavithra , Radha Published a paper titled “a Detailed Analysis Of Different Data Mining Algorithms With Hypothyroid Dataset” In International Journal Of Emerging Technologies And Innovative Research With An Impact Factor Of 5.87 On September 2018.

10. Dhanraj, A.Paithra, Published A Paper Titled “Comparative Study Of Effective Performance Of Association Rule Mining” In Ciit- Data Mining And Knowledge Discovery On May 2018.