

**DEBRE MARKOS UNIVERSITY**

**INSTITIUT OF TECHNOLOGY**

**DEPARTMENT OF INFORMATION**

**TECHNOLOGY**

**RESEARCH PROPOSAL ON CLUSTER BASED NETWORK**

**INTRUSION DETECTION SYSTEM**

**GROUP \_4**

**GROUP MEMBER**

**NO NAME ID**

1. **MELKAMU CHMERE TER/4676/07**
2. **YASSAB AZIZ TER/4696/07**
3. **LAKACHEW YIBELTAL TER/4670/07**
4. **TESFAYE BAIH TER/4691/07**

Table of content

1. Introduction-------------------------------------------------------1
   1. Statement of the research problem --------------------1
   2. Objective of the research--------------------------------2
      1. General objective---------------------------------2
      2. Specific objective---------------------------------2
   3. Hypothesis of the study----------------------------------3
   4. Literature review------------------------------------------3
   5. Scope of the research-------------------------------------3
   6. Methodology of the study--------------------------------3
      1. Interview -------------------------------3
   7. Significance of the research------------------------------4
   8. Conclusion ------------------------------------------------4
   9. Reference ---------------------------------------------------5
2. INTRODUCTION

Recently, many institutions have been experiencing a heavy usage of networks within their systems. However, the broad technological expansion that accompanied these networks has brought along various threats to them. These

threats included many kinds of malicious programmes that affect the efficiency of networks, such as the transmission of data through the network or data that can be accessible via the network. This issue has urged researchers to improve and develop new techniques to explore and contain such threats.

Data mining methods have gained importance in addressing network security issues, including network intrusion detection a challenging task in network security. Intrusion detection systems aim to identify attacks with a high detection rate and a low false alarm rate. Classification-based data mining models for intrusion detection are often in effective in dealing with dynamic changes in intrusion patterns and characteristics. Consequently, unsupervised learning methods have been given a closer look for network intrusion detection. We investigate multiple centroid-based unsupervised clustering algorithms for intrusion detection, and propose a simple yet effective self-labeling heuristic for

detecting attack and normal clusters of network traffic audit data.

**1.2. Statement of the problem**

It is well known that anomaly-based IDS suffer from the high rate of false alarms. Continuous efforts are being made to reduce the high false positive rate. We believe that intrusion detection is a data analysis process and can be studied as a problem of classifying data correctly. From this standpoint, it can also be observed that any classification scheme is as good as the data presented to it as input. More clean the data; higher accurate results are likely to be obtained. From anomaly-based IDS point of view, it implies that if we can extract features that demarcate normal data from abnormal one properly, false positive rate can be reduced to a great extent. Therefore, in this work, we investigate the techniques which facilitate in the process of demarcating normal data from abnormal ones. (1)

1.3. Objective of study

1.3.1. General objective

The general objective of this study is constructing a data mining framework for intrusion detection system that will enhance the network security system.

* + 1. Specific objectives

The objective of this proposal is to present a framework that reduces IDS alerts and assesses its threat. To achieve the above objectives, the following specific objective or procedures will be taken into account:

• Leveraging information gain ratio algorithm to extract the best features of IDS alerts for the purpose of assessing the alerts

• Building a new aggregation IDS alert algorithm to reduce the amount of false positive alerts and to get rid of the alert redundancy

• Developing a multi features based on priory algorithm to find the threat degree of multi features and to assess the threat scores of IDS alert

• Building a visualization engine that involves discovered-based knowledge to assist network engineers in making an appropriate decision

* 1. Research Question /Hypothesis of study

This phase will be built over a proposed new aggregation alert algorithm and it will be done in three stages. The first stage removes any redundant alert based on the similarity of the alert features. The second stage also removes the redundant alert based on similarity of the alert features with threshold value which gives more accuracy result. The final stage of algorithm proposes to remove the false alert based on rules prepared for this purpose.

1.5. Literature review

Intrusion detection system is used to generate alerts, those alerts can be classified into false positives and true negatives. Kruegel and Robertson (2004) developed a

plug-in to add an alert processing pipeline to IDS Snort. Root-cause analysis was proposed by (Julisch and Dacier, 2002) to identify the root causes that trigger false

positives and remove the alert generated. However, this method cannot be controlled. Fixing a problem is also very expensive, thus its impracticality. Pietraszek (2004) adopted a system that worked faster and an effective rule learner, requiring no human feedback and background knowledge. The disadvantage of this system is that it requires infinite growth size to train the system during its lifetime; thus, the system is inefficient. To perform alert verification using the Nessus vulnerability scanner. Astatistical causality analysis correlation approach was

proposed by (Lee and Qin, 2005). This approach was based on statistical analysis and time series to develop attack scenarios. The authors proposed a clustering

technique to aggregate the alerts to be represented as one hyper alert in each cluster based on time intervals. The objective of their approach was to reduce the amount

of alerts and obtain alert prioritization to identify the important alerts. The drawback of this approach is also its incapacity to remove redundant alerts and its

inflexibility to choose the alert features. A robust alert cluster mechanism to reduce false alerts was proposed by (Njogu and Jiawei, 2010). This mechanism calculates the similarities of verified alerts using distance among the new alert features. (2)

1.6. Scope of the research

This proposal is a statement of needs, focusing on cluster based intrusion detection system (IDS) functional and performance requirements. These requirements are grouped into five categories

• Processing requirements

• Functional requirements

• Output requirements

• Technical requirements

• Miscellaneous requirements

Performance requirements are included throughout these categories but are limited in definition since the best of available technology is the capability sought.

1.6.1. Interview

Primary and secondary data gathering tools have advantage to collect the necessary data for the research. Unstructured interview was used as a primary data gathering tool. Unstructured interview is an open situation, having greater flexibility and freedom.

1.7. Significance of the research

Intrusion detection systems offer organizations a number of significant, starting with the ability to identify security incidents. IDS can be used to help analyze the quantity and types of attacks and organizations can use this information to change their security systems or implement more effective controls. An intrusion detection system can also help companies identify bugs or problems with their network device configurations. These metrics can then be used to assess future risks.

* monitoring users and system activity
* auditing system configuration for vulnerabilities and misconfigurations
* assessing the integrity of critical system and data files
* recognizing known attack patterns in system activity
* identifying abnormal activity through statistical analysis
* managing audit trails and highlighting user violation of policy or normal activity
* correcting system configuration errors

**CONCLUSION**

This proposal proposes a new framework called An Ids Alert Reduction and Our framework expect to reduce the false positive alerts and to get rid of the alert redundancy, also to find the threat score of features to assessment the threat score of IDS alerts. This to increase the efficiency of network security and to increase it is accuracy level.

**References**

**[1].**http://shodhganga.inflibnet.ac.in/bitstream/10603/25883/10/10\_chapter%201.pdf

[2].https://pdfs.semanticscholar.org/64e8/b287ce03f343c15c3ffbe8eaeac7495e224d.pdf

Al-Saedi, K.H., H. Al-Khafaji, A. ALmomani, S. Manickam and S. Ramadass, 2011. An approach to assessment of network worm detection using threatening-database.

Elshoush, H.T. and I.M. Osman, 2011. Alert correlation in collaborative intelligent intrusion detection systems-A survey. Applied Soft Comput. J., 11: 4349-4365. DOI: 10.1016/j.asoc.2010.12.004

Maggi, F., M. Matteucci and S. Zanero, 2009. Reducing false positives in anomaly detectors through fuzzy alert aggregation. Inform. Fusion, 10: 300-311. DOI: 10.1016/j.inffus.2009.01.004

M6bile agent in LAN environment”, Proceedings of International Journal of Advanced Research

in Computer and Communication Engineering, Vol. 2, Issue 4, April 2013, pp:1901-1903.