ISSN: 2321-7782 (Online)
Volume 2, Issue 8, August 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

# *Efficient Method for Intrusion Detection and Countermeasure Selection*

**Shilpa S. Dhange**
Computer Department
Rajarshi Shahu College of Engineering
Pune – India

***Abstract:*** ***Now days as the use of computers and networks increases in each area of day to day life, it becomes very vital to provide the security to computers and networks in order to prevent the loss or misuse of private data. In the network security the methodology called Intrusion Detection System (IDS) is frequently used in the domain of network security and hence this is considered as the key research problems to the researchers. There are many techniques and tools for IDSs introduced previously by various researchers, however each methods fails at some extend as the attackers changes their attacking methods on personal computer or networks. The attacked machine in the network is also called as compromised machines which are later used by attacker to compromise all other entire machines in the network. Therefore one need to have efficient method for the detection of such compromised machines in network those are involved in doing the activities like spamming. Recently one method introduced to prevent attacks from the network called NICE (multiphase distributed vulnerability detection, measurement, and countermeasure selection mechanism). However this NICE method originally proposed for virtual network systems in cloud security. The extension to this method which called as Ex-NICE (Extended-NICE) is proposed to mitigate the basic network intrusions like spam zombies attacks. Ex-NICE is not for the virtual network systems, this is a methodology to improve the detection accuracy.***

***Keywords: NICE, Intrusion Detection, Intrusions, Countermeasure Selection, Attack graph model.***

## I. INTRODUCTION

The attacks over the computer systems and network are now day's increases and hence becoming the major threats to private information security and network security. As the unauthorized activities over the network is growing, the use of Intrusion Detection System become very crucial as the existing old methods like firewalls failed to provide the entire security solutions against the different kinds on intrusions. The Intrusion Detection (ID) is key research area in networks and security. The IDS methodology is main approach which is making sure the securing computer networks and information. The real time events as well as intrusion processes becomes possible by using the system like IDS. The main aim of intrusion detection system is to detect the computer attacks efficiently. As introduction, next listed are the main goals of IDS and also called as basic requirements of IDS tools. 1) Detection of attacks, 2) Prevention of attacks, 3) Detection of policy violations, 4) Enforcement of use policies, 5) Enforcement of connection policies, 6) Collection of evidence etc.

For detection of intrusions each IDS needs to perform the operations like: 1) the examination of manual log, 2) examination of automated log, 3) tool for host-based intrusion detection, 4) Network-based intrusion detection software, 5) System structure and fault audit, 6) Audit tracing management of operating system and recognition of users behavior against security policy of an organization, 7) Statistics analysis of abnormal activities, 8) Monitoring and analyzing user and system activities, 9) Recognition activity model for identification of known attack and generates the alarm as an indication of attack, 10) Measuring the confidentiality and integrity of the system and data files.

 

Formally we can define the term intrusion is nothing but the process of compromising the computer system. And the methodology which is used to identify compromised systems or the attempts those are made to compromise the systems is known as Intrusion Detection.

As the name of IDS indicates, the IDS methods are detect all possible intrusions. The goal of IDS tools is to detect computer attack or illegal access, and to alert the concerned people about the detection or security breach. An IDS install on a network can be viewed as a burglar alarm system installed in a house. Through their methods are different, both detect when an intruder/attacker/burglar is present, and both subsequently issue some type of warning signal or alert [1]., detect, Monitor and respond to any unauthorized activity are the adages of Intrusion detection systems. Network attacks such as DoS attacks can be detected by monitoring the network traffic. There are two basic types of intrusion detection: Network-based and Host-based. Each has a distinct approach to securing data and monitoring, and each has distinct advantages and disadvantages. *Host-based intrusion detection systems* (HIDS) are IDSs that operate on a single workstation. HIDS monitor traffic on its host machine by utilizing the resource of its host to detect attacks. [2] *Network-based intrusion detection systems* (NIDS) are IDS that operate as stand-alone devices on a network. NIDS monitor traffic on the network to detect attack such as denial of service attack; port scans or even attempts to crack into computers by monitoring network traffic [2].

The existing IDS methods which are based on use of distributed acquisition methods, centralized processing methods, hierarchical processing methods. Such IDS designs later suffered from few limitations mainly in the concentrated analysis of components with higher loading may become the chock point of IDS and lead to the failure of the single point.

From our recent study over the concepts of NICE in [1], authors presented the new method for detecting and preventing the network intrusions like DDoS (Distributed Denial-of-Service) attacks. The involvement of DDoS attacks is generally presented at initial stage activities such as low frequency scanning of vulnerability, multistep exploitation, at last the DDoS attacks via the compromised machines. NICE approach is specially subjected to use with virtual machine networks in cloud security. This system is suffered from few limitations such as the accuracy of attacks detection is poor, the scalability of NICE needs to be investigated further for distributed as well as centralized networks. Here we are presenting the extended version of NICE with improving the detection accuracy. The proposed approach is called as Extended-NICE (Ex-NICE). The proposed Ex-NICE method is based only on host computer rather than virtual machine or cloud security concepts as per given in [1]. Thus Ex-NICE is purely the network based IDS system in which we can incorporate the concepts and algorithms of NICE [1] for the detection and prevention of different kinds of attacks over the computer or network. For experimental study the real time IDS data called NSL-KDD dataset. In next section II presents literature survey different approaches presented over the IDS. In section III, the proposed approach and its system block diagram is depicted. In section IV presenting the current state of implementation and results achieved. Finally conclusion and future work is predicted in section V.

## II. LITERATURE SURVEY

The main source of intrusion, attacks, malicious activities are Internet now days, and its does especially through the web applications. The worms in the Internet spread over computer networks through the activities like attacking, searching as well as automatically infecting the remote machines. Therefore such kinds of intrusions are now days become growing threats for secured information. To provide the security against such intrusions in network is that to identify the different properties of virus in which the impact of patching is included, awareness of other human countermeasures and the impact of network traffic, even the ways how these malicious codes reside in a certain hosts, etc. In this section we are listing out different methods presented by various authors for IDS in different domains.

Gu et al. [2] proposed architecture of combining multiagent systems and dendritic cells. Most AIS researches focus on the development of specialized AIS algorithms inspired by theories such as the negative selection theory or the danger theory. Applying AIS algorithm to IDS can be traced back to [3].

 

Greensmith et al. [4] employed dendritic cells (DCs) within AIS which coordinate T-cell immune responses.

Kim et al. [5] proposed "CARDINAL" which embedded T-cell process within the danger-theory-based AIS.

Greensmith et al. [4], [6] proposed the Dendritic Cell Algorithm (DCA) whose purpose is to correlate data in the form of antigens and signals, then to identify groups of antigens as normal or anomalous. DCA achieves such missions through a generation of an anomaly coefficients, namely, *mature context antigen value (MCAV)*. It is believed that a DC is better performed by agent technology while considering its adoption to network environment.

Wheeler P. *et al*. [7] proposed to use a distributed system where in which each node has the same rules. The packets are sent to each node using load balancer. Thus, each node will receive 1/N from original load, where N is the number of nodes.

Sanz-Bobi *M. A. et al*. [8] proposed an intelligent system for automatic detection of intrusions in computer networks (Intrusion Detection System based on Artificial Intelligence IDSAI). Its architecture is based on the multi-agent system in which several types of agents cooperate together to perform a fast and reliable detection of intrusions.

Schuff D. L. *et al*. [9] proposed Snort 2.6 version based method for IDS. It only execute multiple instance of original Snort in parallel and use load balancer that distribute task queues to dispatch traffic. After distributing task by load balancer, each processing threads does a job, such as decode, preprocess, and detects.

Yoshioka A. *et al*. [10] presented generates a hash value using five protocol fields for each rule. The five protocol fields are source IP, destination IP, source port, protocol type, and destination port. Each hash value is stored in a single hash table. When a packet arrives, the same hash function is applied to the incoming packet and the hash value generated from the packet is used to search in the hash table for the matching rules. This approach searche to the matching rule multiple times against each packet to cover all possibilities.

In [11], Multi-layer intrusion detection model was proposed. They used gain ratio for selecting the best features for each layer and classified the system by using machine learning algorithms such as C5.0, Multi-Layer Perceptron (MLP) Neural Networks and Naïve Bayes.

In [12] authors proposed a three-layer approach to enhance the perception of intrusion detection on reduced feature set to detect both known and novel attacks. They used NSL-KDD data set for their experiment. They employed domain knowledge and the Backward Sequential Elimination (BSE) to identify the important set of features and Naïve Bayes classifier for classification.

In [13], authors used Naïve Bayesian for classification. Their experiment is implemented on NSL-KDD dataset.

## III. Proposed Approach Framework and Design

### 3.1 Design

The proposed architecture is explained as shown in figure given below.

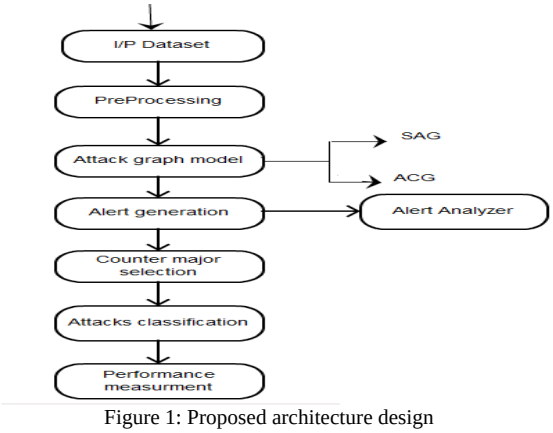


Figure 1: Proposed architecture design

 

### 3.2 Proposed Work

There are many methods presented different authors for IDS with main objective of robust security method and improved detection accuracy. However these methods are doesn't not actually practically test with real time IDS datasets like KDD or Bro. Hence in our proposed approach is the extension to NICE method which called as Ex-NICE (Extended-NICE) which is proposed to mitigate the basic network intrusion attacks. Ex-NICE is not for the virtual network systems. Ex-NICE methodology improves the detection accuracy using Naïve Bayes classification and NSL-KDD dataset is used for experiment.

### 3.3 Algorithm

**Algorithm:**

Step 1: Input dataset called NSL-KDD Intrusion Detection Dataset to the system.

Dataset contains set of fields which contains attack related information.

Step 2: Preprocess dataset.

In pre-processing, unwanted symbol,null values are removed from both testing and training dataset before processing.

Step 3: A new alert is mapped to their respective nodes in SAG.

An SAG is a tuple.

SAG=(V,E) where

V denotes set of vertices.

E denotes set of directed edges.

Step 4: Select best countermeasure based on ROI.

$$ROI[t,cm]=\frac{benefit[t,cm]}{cost.cm+intrusiveness.cm}$$

Where, t=Node in SAG.

cm=Countermeasure.

benefit=ΔPr ($target\ node$). Where Pr is probability.

cost.cm=cost of countermeasure.

intrusiveness.cm=intrusiveness.cm.

Step 5: Classify attack and normal packets using Naive Bayes classifier.

$$\text{Attack Probability}=\frac{\text{Number of Attack Packets}}{\text{Total Number of Packets}}$$

Step 6: Measure performance by calculating accuracy.

$$\text{Accuracy}=\frac{(TP+FP)}{(TP+FP+TN+FN)}$$

Where, TP = True positive

FP = False positive

TN = True negative

FN = False negative

 

For alert generation we use alert co relation algorithm and attribute classification is computed as in [12].

## IV. WORK DONE

### 4.1 Input:

The NSL-KDD dataset consists of selected records of the complete KDD data set and has advantages over the original KDD data set. The dataset is divided into two parts as training and test dataset. Training is used to train the work presented, while test dataset is used to test it. Test dataset contains additional attacks which are not described in training dataset.

### 4.2 Hardware and Software Used

**Hardware Configuration**

- Processor - Pentium –IV
- Speed - 1.1 Ghz
- RAM - 256 MB(min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Monitor - SVGA

**Software Configuration**

- Operating System - Windows XP/7/8
- Programming Language - Java
- Tool - NetBeans.

### 4.3 Matrix computation

In this paper we compute matrix according to evaluation security provided. This matrix is needed in alert graph generation technique in [1].

### 4.4 Results of work done

Following graph shows the performance of implemented system. As it shows, the accuracy rate of our implementation in percentage.

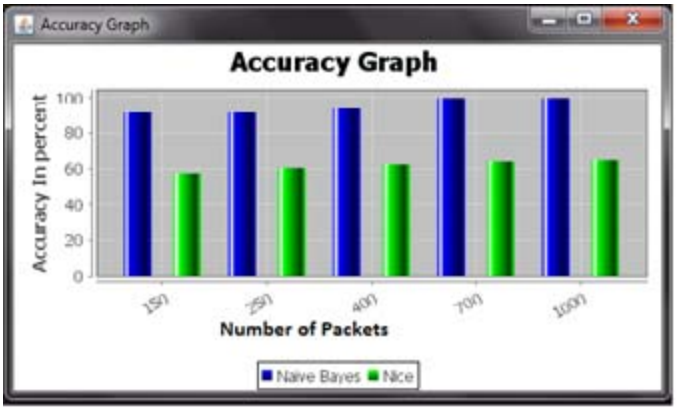


Figure 2: Performance measurement

 

## V. Conclusion and Future Work

Providing the security to personal information as well as computer networks is becoming the challenging research problem. Proposed system is the new IDS approach for mitigating the different kinds of intrusions or attacks on network based on concepts used in NICE. Presented Ex-NICE is targeted to work under computer networks only rather than virtual distributed networks in cloud security. The proposed method first compute the attack graph model as per given in NICE and based on it features are selected for the alert generation. Finally the countermeasures are selected based on generated alerts. The practical work is done using the real time dataset called NSL-KDD which is consisting of different kinds of attacks. From experimental results, it is clear that proposed approach improves the accuracy of detecting and mitigating the attacks in network as compared to NICE. For the future work, the proposed method can suggest to investigate under real time network settings.

## References

1. Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang, “NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems”, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013.
2. F. Gu, U. Aickelin, and J. Greensmith, “An agent-based classification model,” in 9th European Agent Systems Summer School (EASSS2007), 2007.
3. U. Aickelin, P. Bentley, S. Cayzer, and J. Kim, “Danger theory: The link between ais and ids,” Lecture Notes in Computer Sciences, vol. 2787,pp. 144–165, 2003.
4. J. Greensmith, J. Feyereisl, and U. Aickelin, “The dca: Some comparison,” Evolutionary Intelligence, vol. 1, no. 2, pp. 85–112, 2008.
5. Kim, An Artificial Immune System Architecture for Computer Security Applications. New York: John Wiley and Sons, 1978.
6. J. GreensmithU, Aickelin, and S. Cayzer, “Detecting danger: The dendritic cell algorithm,” Robust Intelligent Systems, vol. 12, pp. 89–112, 2008.
7. Wheeler P., and Fulp E. W., “A taxonomy of parallel techniques for intrusion detection”, In Proceedings of the 45th Annual Southeast ACM Regional Conference, Winston-Salem, North Carolina, USA, P.P 278-282,2007.
8. Sanz-Bobi M. A., Castro M., and Santos J., "IDSAI: A Distributed System or Intrusion Detection Based on Intelligent Agents," In Proceedings of the Fifth International Conference on Internet Monitoring and Protection, pp.1-6, 2010.
9. Schuff D. L., Choe Y. R., and Pai V. S., “Conservative vs. optimistic parallelization of stateful network intrusion detection,” in proceeding of the 12th ACM SIGPLAN symposium on Principals and Practice of parallel programming, 2007.
10. Yoshioka A., Shaikot S. H., and Kim M. S., “Rule Hashing for Efficient Packet Classification in Network Intrusion Detection,” In Proceeding of the Computer Communications and Networks, 2008. ICCCN '08. Proceedings of 17th International Conference on.
11. Ibrahim H.E., Badr S.M, Shaheen M.A, “Adaptive Layered Approach using Machine Learning Techniques with Gain Ratio for Intrusion Detection Systems”, International Journal of Computer Applications (0975 – 8887) Volume 56– No.7, October 2012.
12. Sharma el N., Mukherjee S.,” A LAYERED APPROACH TO ENHANCE DETECTION OF NOVEL ATTACKS IN IDS”, International Journal of Advances in Engineering & Technology, Sept 2012.
13. Jain M., Richariya V. “An Improved Techniques Based on Naive Bayesian for Attack Detection”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 1, January 2012.

## Author(s) Profile


**Shilpa Dhange** received the B.E. degree in Computer Science and engineering from SVERI’s college of engineering, Pandharpur, Solapur university**.**

 