INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 1, Issue 1, OCTOBER 2015.

REVIEW OF IDS SYSTEM IN LARGE SCALE ADHOC NETWORKS

Palamdeep[a,*], Dr.Parminder Singh[b]

[a] *MTech Student, k.palambrar@gmail.com,Chandigarh Engineering College,Landran,Punjab,India*
[b] *Assistant Professor, singh.parminder06@gmail.com,Chandigarh Engineering College,Landran,Punjab,India*

ABSTRACT

There are a number of threats that violate the security policies and breaches all over network. This has happened when malicious node present on the network; it may be present on one or more node that detect the pattern of the packet or frame and the misuse the information. In this paper we detect the network based attack and our proposed methodology detect suspicious activity, it respond when any wrong information enter in the log or any even occurred. Depending on conditions we fix the threshold value that alarms it when any suspicious activity occurred. If the value goes higher at certain level then our system disconnect the suspicious node and send reply to all the authenticate nodes. The proposed approach has been working in Mobile Ad Hoc networks (MANETs) and detecting bidirectional traffic; the bidirectional traffic can be configuring in access point out of this we used an infrastructure approach to identify the intrusion.

I. INTRODUCTION

An Intrusion Detection System (IDS) is responsible for performing IntrusionDetection within a system. However, Distributed Intrusion Detection System responsible for detecting distributed attacksrequires components that spread across different networks which build thedistributed environment.Intrusion detection systems are usually classified as host-based or network-based [3]. The instruction based detection has been shown in the figure 1 and this system specified the internal working of server, firewall and routers. The IDS system which we deployed in the network scenario could be verified every activity and traffic; the traffic may be inbound or outbound because we used bidirectional traffic. This traffic would be verified only in the adjacently devices; the log based file had created by the IDS system and reported to router and firewall so if any suspicious activity performing on the network based system, it alarms and

terminated connection by the main router that would be treated as Master-Router or Border Router that directly communicates with the Public Network.

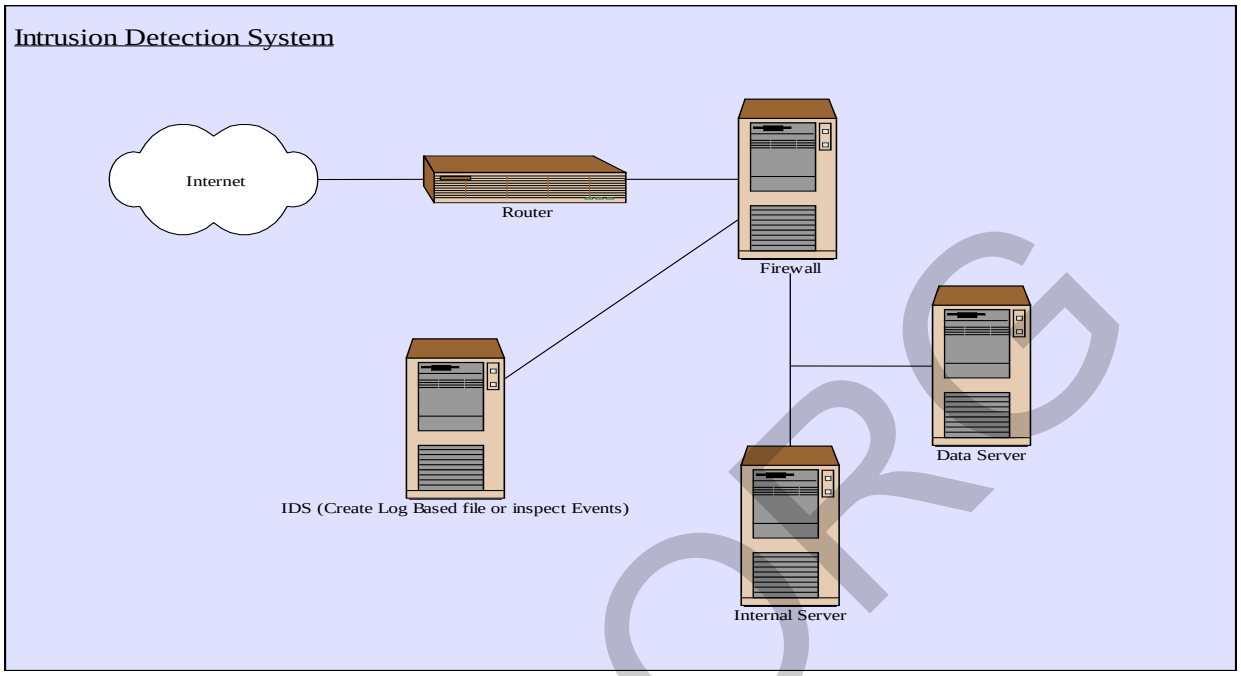

Fig. 1. Intrusion Detection System

a) Characteristics of IDS Based System

The following characteristics are ideally desirable for an intrusion detection system(based on the list provided by [2]):

1. It must run continually with minimal human supervision.

2. It must be fault tolerant:

(a) The intrusion detection system must be able to recover from system crashes,either accidental or caused by malicious activity.

(b) After a crash, the intrusion detection system must be able to recover its previousstate and resume its operation unaffected.

II. RELATED WORK

In [1] introducing threetypes of internal attack named as Node isolation, routedisruption, Resource consumption and presented an approach tohandle such type of internal attacks for wireless network.The proposed work can beperformed by modifying ad-hoc on demand distance vectorrouting protocol. The simulation experiments are conducted onNS-2 environment in Linux platform.The recovery procedure hasalso been discussed for the MANET under various attacks. Therecovery has been provided by finding the attacker node andisolating that particular node from the network topology.In [8], the paper proposed architecturefor a distributed and cooperative intrusion detection systemfor ad-hoc networks based on statistical anomaly detectiontechniques but they have not properly mentioned about thesimulation scenario and the type of mobility they have used.Second, intrusion detection in MANET must be carried outin a distributed fashion because of the absence of infrastructureand mixed topology.In [9], A. Mishra emphasizes the challenge for intrusiondetection in ad-hoc network and purpose the use of anomaly detection, but do not provide a detailed solution orimplementation for the problem.Distributed Intrusion Detection System describes the advantages [10], and further improved the detection system of multi agent viz accuracy anddetection speed, and enhance the system's own security.

III. PROBLEM DEFINITION AND FORMULATION:

Intrusion detection is a new and rapidly developing area and it has become an important issue in network security. Intrusion detection systems are hardware or software mechanisms that detect and logs inappropriate, incorrect, or anomalous activity for further investigation. Network-based Intrusion Detection System is almost powerless for complex attacks.Attacks by intruderscause unauthorized use of wireless network so that the whole network will be suffered from packet loses[1].The goal of this paperis to providing a methodology to detect network based attacks with incomplete audit data. This proposed work has proposed a technique which will find intruders by monitoring the network traffic and creation of per-flow network traces. It also aims to design an adaptive learning of intrusion.

IV. METHODOLOGY/ PLANNING OF WORK

The following Methodology has been planned out in the network scenario; discussed in figure 1.

- Create a Network Scenario of Mobile AdHoc Networks (MANETs).
- Establish the desired conditions in the computing environment;
- Start the IDS;
- Run the TCL scripts; and
- Analyze the IDS's output.

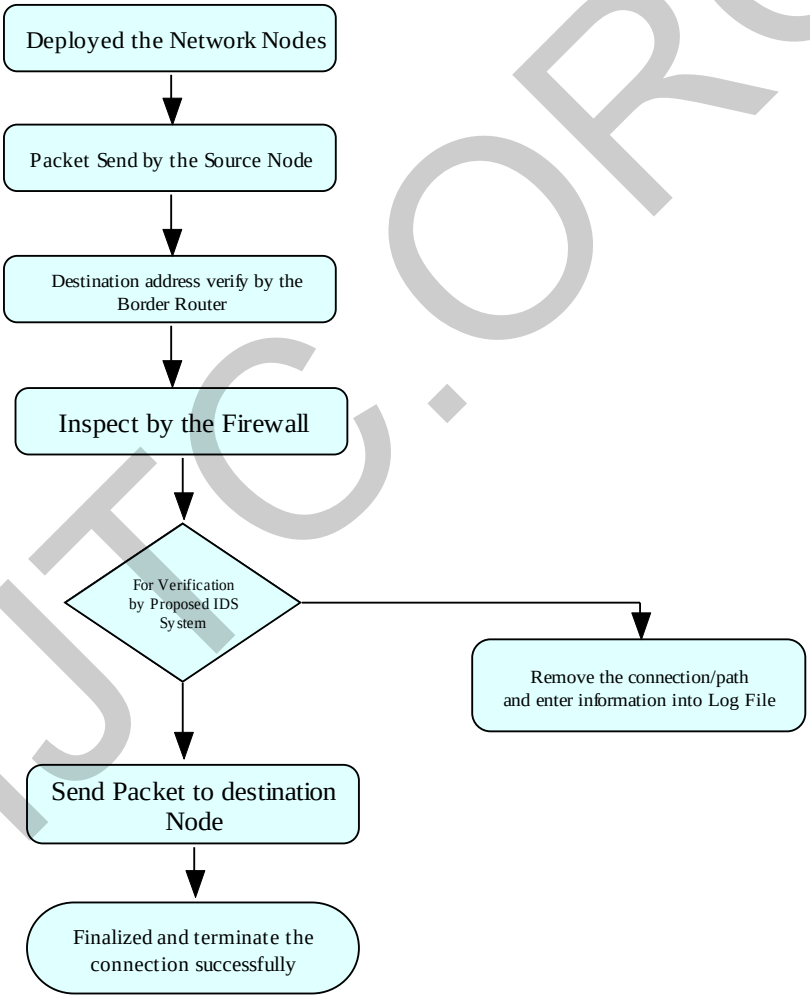

Fig.2. Flow Chart of Proposed IDS System

V. CONCLUSION

The proposed IDS system will be implementing on the large scale network and this network find out the malicious nodes and remove or disconnect the path from the current network scenario. This network support border router and firewall and manage the log information effectively. This paper explores the network based attack which is harmful for present network and extracts any kind of information. The aim of this paper is to find these attacks and mitigate it.

REFERENCES

[1] S.S.Chopade, N.N.Mhala, “A Co-Operative Intrusion Detection System inMobile Ad-Hoc Network”,International Journal of Computer Applications", volume 18, No.6,2011,pp.34-39

[2] Mark Crosbie and Gene Spafford. Active defense of a computer systemusing autonomous agents. Technical Report 95-008, COAST Group, Departmentof Computer Sciences, Purdue University, West Lafayette, Indiana,February 1995. URL http://www.cerias.purdue.edu/homes/spaf/tech-reps/9508.ps.

[3] Biswanath Mukherjee, Todd L. Heberlein, and Karl N. Levitt. Network intrusiondetection. IEEE Network, 8(3):26–41, May/June 1994.

[4] HakanKvarnstrom. A Survey of Commercial tools for Intrusion Detection.Technical Report 99-8, Dept. of Computer Engineering, Chalmers University ofTechnology, Sweden.

[5]MeeraGandhi,S.K.Srivatsa,"Detecting and preventing attacks using network intrusiondetection systems",International Journal of Computer Science and Security, Volume 2,2011

[6]YianHuang,WenkeLee,"A Cooperative Intrusion Detection System for Ad HocNetworks",International journal of computer applications, 2011.

[7]S. Jacobs, S. Glass, T. Hiller, and C. Perkins, “Mobile IPauthentication, authorization, and accounting requirements,” Requestfor Comments 2977, Internet Engineering Task Force, October 2000.

[8] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniquesfor Mobile Wireless Networks," ACM J. Wireless Networks, pp. 545-556, 2003.

[9] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection inWireless Ad-Hoc Networks," in IEEE Wireless Communications, pp.48- 60, February 2004.

[10]WeijianHuang,YanAn and Wei Du,"A Multi-Agent-Based Distributed Intrusion Detection System",International Conference on Advanced Computer Theory and Engineering (ICACTE),2010.

[11]Richard Power. 1999 CSI/FBI computer crime and security survey. Computer SecurityJournal, Volume XV(2), 1999.

[12]Teresa F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. G. Neumann, H. S. Javitz, A. Valdes, and T. D. Garvey. A real-time intrusion detection expert system (IDES)– final technical report. Technical report, SRI Computer Science Laboratory, SRIInternational, Menlo Park, California, February 1992.