

ANALYSING THE ENHANCED INTRUSION DETECTION SYSTEM

¹Pankaj, ²Mr. Puneet Garg

¹ M.Tech Student, Ganga Institute of Technology and Management, kablana (Jhajjar)

pk2235@gmail.com

² Assistant Professor, Ganga Institute of Technology and Management, kablana (Jhajjar)

puneet.gitam@gmail.com

Abstract

There had been need to focus on Establishment of Network Environment to test flow of packets & also need of Development of packet sender & receiver module. We had studied of existing Testing transmission delay in packet transmission & Testing processing delay during packet transmission. We also make study of testing queuing delay of network packets.

An Intrusion Prevention System is a network security/threat prevention technology that audits network traffic flows to detect & prevent vulnerability exploits. There are two types of prevention system they are Network & Host.

Keywords: Intrusion Prevention System, Transmission, Packets.

1. Introduction

An IDS is referred as burglar alarm. For example, lock system in house protects house from theft. But if somebody breaks lock system & tries to enter into house, it is burglar alarm that detects that lock has been broken & alerts owner by raising an alarm.

Moreover, Firewalls do a very good job of filtering incoming traffic from Internet to circumvent firewall. For example, external users could connect to Intranet by dialling through a modem installed in private network of organization; this kind of access cannot be detected by firewall. An Intrusion Prevention System (IPS) is a network security/threat prevention technology that audits network traffic flows to detect & prevent vulnerability exploits.

FUNCTIONS OF IDS

The IDS consist of four key functions namely, data collection, feature selection, analysis and Action.

Data collection

This module passes data as input to IDS. Data is recorded into a file & then it is analysed. Network based IDS collects & alters data packets & in host based IDS collects details like usage of disk & processes of system.

Feature Selection

To select particular feature large data is available in network & they are usually evaluated for intrusion. For example, Internet Protocol (IP) address of source & target system, protocol type, header length & size could be taken as a key for intrusion.

Analysis

The data is analysed to find correctness. Rule based IDS analyse data where incoming traffic is checked against predefined signature or pattern. Another method is anomaly based IDS where system behaviour is studied & mathematical models are employed to it.

Action

It defines about attack & reaction of system. It could either inform system administrator within all required data through email/alarm icons or it could play an active part in system by dropping packets so that it does not enter system or close ports.

2. LITRATURE REVIEW

Nilotpal Chakra borty (2013) "intrusion detection system & intrusion prevention system: a comparative study" [1] Intrusions in computing environment are a very common undesired malicious activity that is going on since inception of computing resources Within whole world

depending on computers, being directly or indirectly, it is a very important issue to prevent malicious. A number of security measures have taken place for last three decades, but as Technology had grown up, so as security threats activities & threats that could hamper computing infrastructures. Intrusion Detection System (IDS) & Intrusion Prevention System (IPS) are standard measures to secure computing resources mostly in a network.

B.Santos Kumar (2013) "Intrusion Detection System- Types & Prevention" [2]

Intrusion detection is act of detecting unwanted traffic on a network or a device. An IDS could be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity & events such as illegal & malicious traffic, traffic that violates security policy, & traffic that violates acceptable use policies.

Dr. S.Vijayarani (2015) "intrusion detection system – a study"[3] Intrusion Detection System (IDS) is meant to be a software application which monitors network or system activities & finds if any malicious operations occur. Tremendous growth & usage of internet raises concerns about how to protect & communicate digital information in a safe manner. Nowadays, hackers use different types of attacks for getting valuable information. Many intrusion detection techniques, methods & algorithms help to detect these attacks.

R Rangadurai Karthick (2012) Adaptive Network Intrusion Detection System using a Hybrid Approach

Any activity aimed at disrupting a service or making a resource unavailable or gaining unauthorized access could be termed as an intrusion. Examples include buffer overflow attacks, flooding attacks, system break-ins, etc. Intrusion detection systems (IDSs) play a key role in detecting such malicious activities & enable administrators in securing network systems. Two key criteria should be met by IDS for it to be effective: (i) ability to detect unknown attack types, (ii) having very less miss classification rate.

3. TOOLS AND TECHNOLOGY

An intrusion detection product available today addresses a range of organizational security goals. This section discusses about security tools.

SNORT

Snort is lightweight & open source software. Snort uses a flexible rule-based language to describe traffic. From an IP address; it records packet in human readable form. Through protocol analysis, content searching, & various pre-processors Snort detects thousands of worms, vulnerability exploit attempts, port scans, & other suspicious behaviour.

OSSEC-HIDS

OSSEC (open source security) is free open source software. It would run on major operating system & uses a Client/Server based architecture. OSSEC has ability to send OS logs to server for analysis & storage. It is used in powerful log analysis engine, ISPs, universities & data centres. Authentication logs, firewalls are monitored & analysed by HIDS.

FRAGROUTE

It is termed as fragmenting router. Here, from attacker to frag router IP packet is sent and they are then fragmented & transformed to party.

HONEYD

Honeyd is a tool that creates virtual hosts on network [6]. The services are used by host Honeyd allows a single host to request multiple addresses on a LAN for networks simulation. It is possible to knock virtual machines or to trace route them [6]. Any type of service on virtual machine can be simulated according to a simple configuration file [6].

KISMET

It is a guideline for WIDS (Wireless intrusion detection system). WIDS compromises within packet payload & happenings of WIDS. It would find burglar access point.

MATLAB

Mat lab As a Simulation Tool

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, & programming in an easy-to-use environment where problems & solutions are expressed in familiar mathematical notation. Typical uses include: Math & computation.

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment & fourth-generation programming language. Developed by

Math Works, MATLAB allows matrix manipulations, plotting of functions & data, implementation of algorithms, creation of user interfaces, & interfacing within programs written in other languages, including C, C++, Java, Fortran & Python.

4. PROBLEM STATEMENT

In case of Intrusion detection there are several problems with existing system. Usually data is transferred from one IP to another IP using most commonly used protocol such as FTP, TELNET, HTTP.

Second thing is that the probability of success of attack increases when data is large in size and sent as it is. So, we have reduced the size of packets by exchanging contents of data file with some short words during send and original words are restored at receiving end.

If huge Number of packets sent on common route then it becomes difficult to save data from intrusion detection attack.

Third option is to reduce the number of packets in queue so that during routing it becomes easy to secure the packets from intrusion detection.

5. IMPLEMENTATION

Server Side Implementation

In this project we have developed a server application as well as client application in Net bean IDE. As shown in following figure:

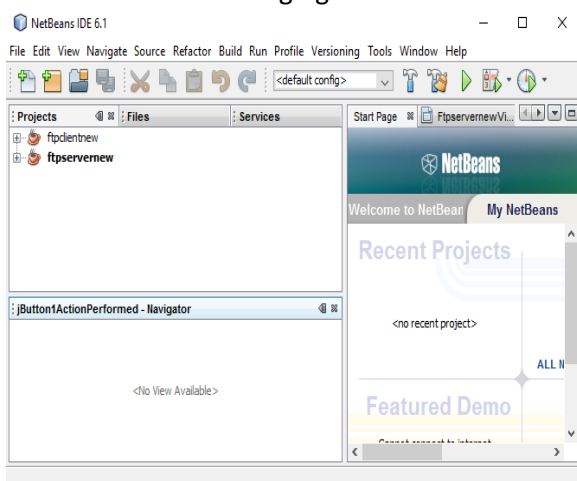


Figure 1: In server side we have made designing and written code to enable download option and disable download option

Client side implementation

Following is the design view for file client in order to upload and download data. Here we have to specify

port no, file path, ip address of server and token (to encode data)

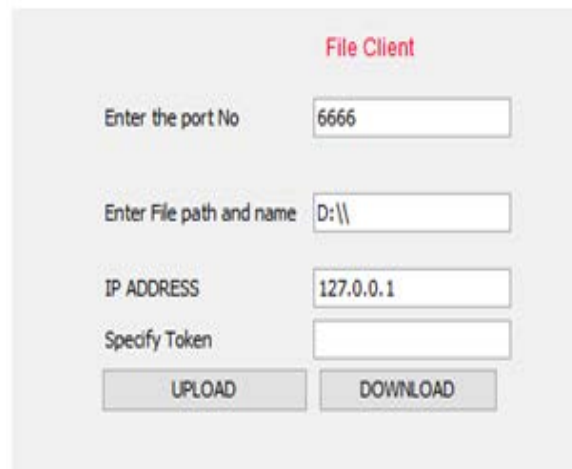


Figure 2: Code to implement UPLOAD on client side Result of output

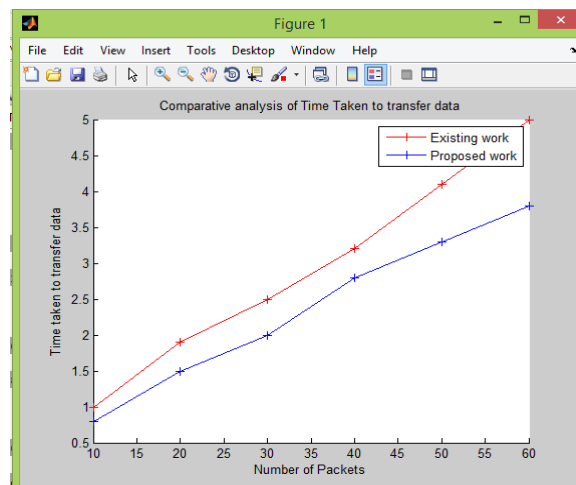


Figure 3: Comparative analysis of time taken to transfer packet

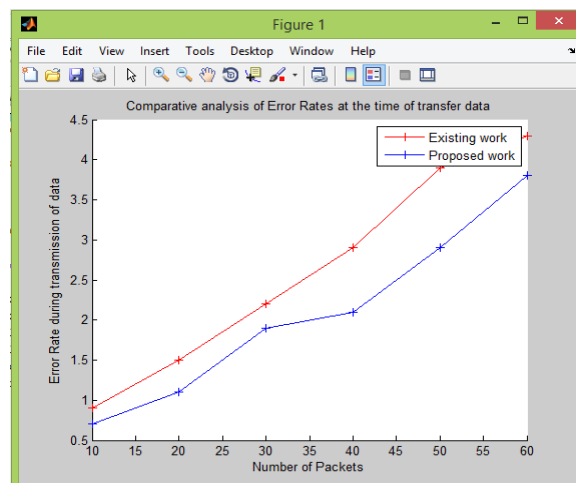


Figure 4: Comparative analysis of error rates at the time of transfer data

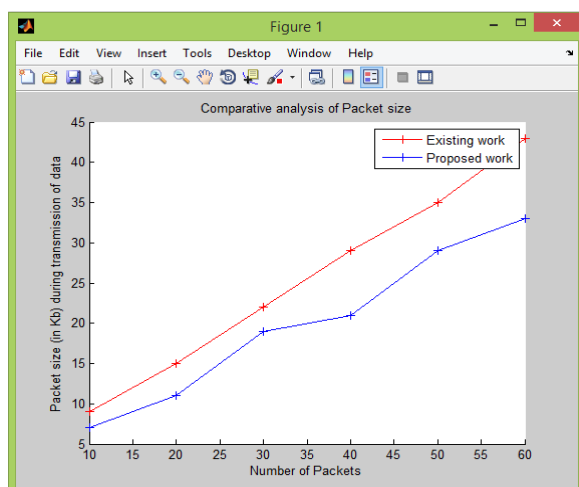


Figure 5: Comparative analysis of packet size

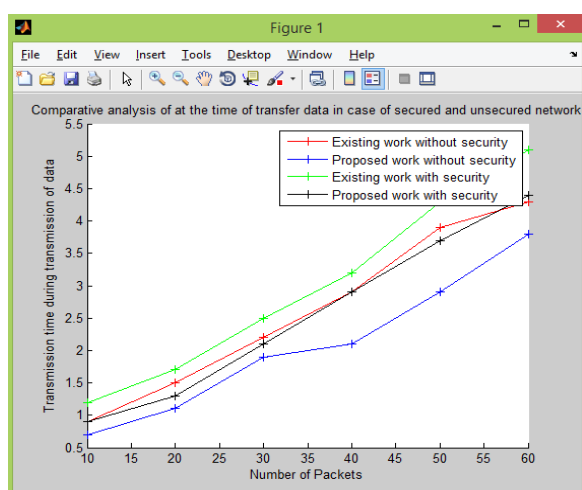


Figure 6: Comparative analysis of transmission time in case of secure and unsecured traditional and proposed work

6. FUTURE WORK

The presented work is about to improve the routing in MANET by using the concept of IDS mechanism which can provide security as required and also increase the overall life time of the network by decreasing the energy consumption by the node is required. For optimum the local node we divide the network in smaller zones and identify the virtual coordinator over the zone. This coordinator will contain the communication statistics of zone nodes. As the routing will be performed, the effective hop selection will be done by the virtual coordinator.

7. CONCLUSION

Our approach also provides practical advantages over many existing techniques whose application requires customized & complex runtime environments: It is defined at application level,

requires no modification of runtime system, & imposes a low execution overhead.

We are focusing on following objectives. So, there had been need to focus on Establishment of Network Environment to test flow of packets & also need of Development of packet sender & receiver module. We had studied of existing Testing transmission delay in packet transmission & Testing processing delay during packet transmission. We also make study of testing queuing delay of network packets.

7. REFERENCES

1. Nilotpal Chakra borty(2013) "intrusion detection system and intrusion prevention system: a comparative study" International Journal of Computing and Business Research (IJCBR) Volume 4 Issue 2 May 2013
2. B.Santos Kumar(2013) "Intrusion Detection System- Types and Prevention" International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013
3. Dr. S.Vijayarani (2015) "INTRUSION DETECTION SYSTEM – A STUDY" International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015
4. E. Ahmed, K. Samad, and W. Mahmood, "Cluster-based intrusion detection (cbid) architecture for mobile ad hoc networks," in 5th Conference, AusCERT2006 Gold Coast, Australia, May 2006 Proceedings, 2006.
5. T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," in Wireless Network Security, pp. 159–180, Springer, 2007.
6. P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks," in Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on, pp. 368–373, IEEE, 2003.
7. M. Ngadi, A. H. Abdullah, S. Mandala, et al., "A survey on manet intrusion detection," International Journal of Computer Science and Security, vol. 2, no. 1, pp. 1–11, 2008.
8. A. Nadeem and M. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," 2012.
9. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges

- and solutions,” *Wireless Communications*, IEEE, vol. 11, no. 1, pp. 38–47, 2004.
10. B. Sun, L. Osborne, Y. Xiao, and S. Guizani, “Intrusion detection techniques in mobile ad hoc and wireless sensor networks,” *Wireless Communications*, IEEE, vol. 14, no. 5, pp. 56–63, 2007.
 11. Y. Li and J. Wei, “Guidelines on selecting intrusion detection methods in manet,” in *The 21st annual conference for information systems educators (ISECON)*, Rhode Island, USA, pp. 4–7, 2004.
 12. L. Bononi and C. Tacconi, “A wireless intrusion detection system for secure clustering and routing in ad hoc networks,” in *Information Security*, pp. 398–414, Springer, 2006.
 13. Z. Xing, L. Grunewald, and K. Phang, “A robust clustering algorithm for mobile ad-hoc networks,” *Handbook of Research on Next Generation Mobile Networks and Ubiquitous Computing*, pp. 187–200, 2008.
 14. B. Kisku and R. Datta, “An energy efficient scheduling scheme for intrusion detection system in mobile ad-hoc networks,” in *Parallel Distributed and Grid Computing (PDGC)*, 2012 2nd IEEE International Conference on, pp. 1–6, IEEE, 2012.