© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 05 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

IMPLEMENTATION ON INTRUSION DETECTION SYSTEM IN MOBILE COMPUTING

Pooja[1], Shilpa[2]
[1]Reasearch Scholar, Department of COMPUTER SCIENCE &ENGINEERING, Choudhaary Bhim Singh institute of science & technology, pooja16591@gmail.com

[2] Assistant professor, Department of COMPUTER SCIENCE &ENGINEERING, Choudhaary Bhim Singh institute of science & technology, shilpakhurana04@gmail.com

Abstract: - 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. 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.
Keyword: - 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 dialing 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.

[2] 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 analyzed. Network based IDS collects & alters data packets & in host based IDS collects details like usage of disk & processes of system.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 05 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

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 analyzed to find correctness. Rule based IDS analyze data where incoming traffic is checked against predefined signature or pattern. Another method is anomaly based IDS where system behavior 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 .

[3] 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.

[4] 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:

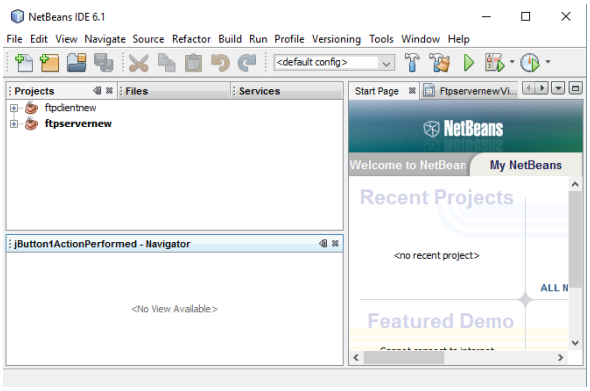

Fig: 1 In server side we have made designing and written code to enable

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 05 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

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)

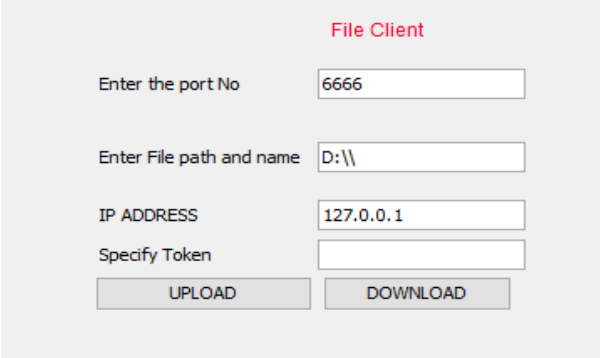

Fig: 2 Code to implement UPLOAD on client side

Result of output

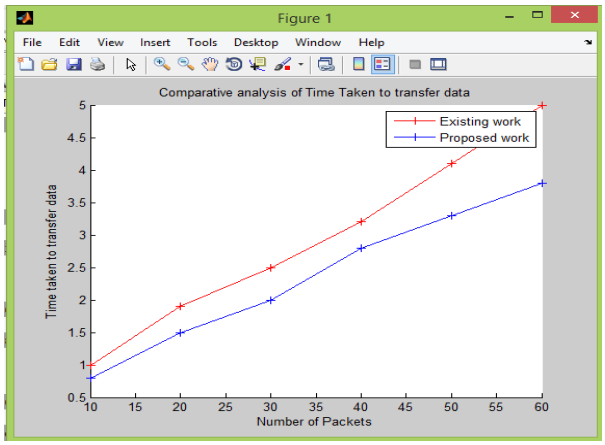

Fig 3 Comparative analysis of time taken to transfer packet

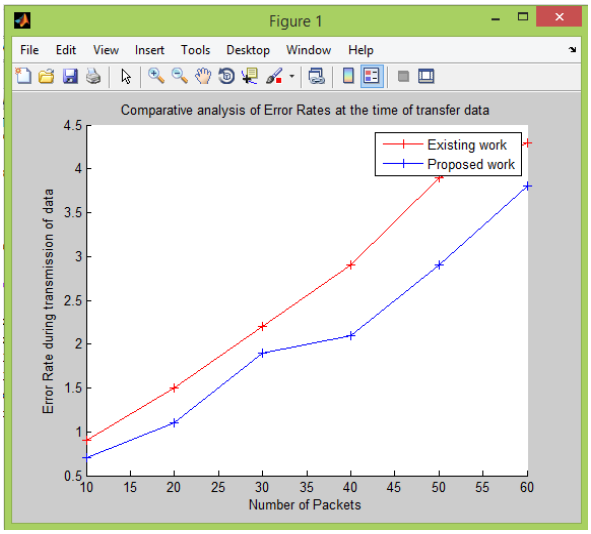

Fig 4 Comparative analysis of error rates at the time of transfer data

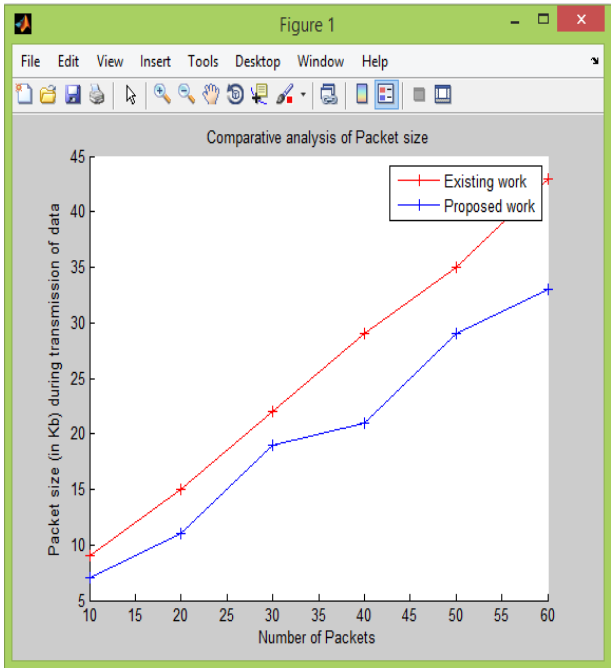

Fig 5 Comparative analysis of packet size

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 05 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

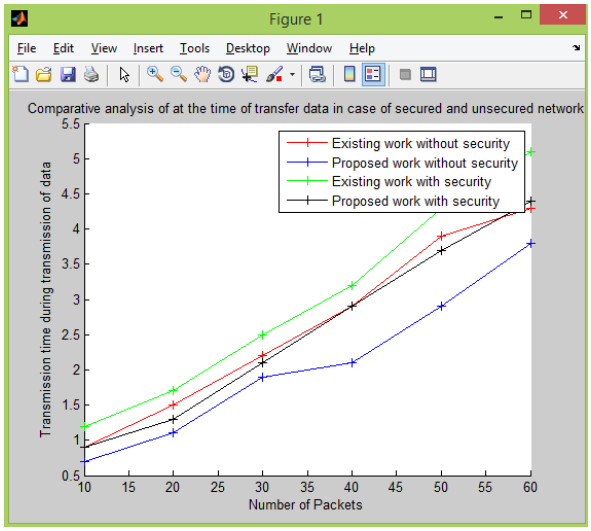

Fig 6 Comparative analysis of transmission time in case of secure and unsecured traditional and proposed work

[5] 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.

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 n etworks," 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.