Review on Intrusion detection system in centralised network

Pankaj[1], Puneet garg[2]

[1]M.Tech. Student ,Computer Science & Engineering

Ganga Institute of Technology and Management Kablana, Jhajjar, Haryana, India

[2] *Associate Professor*, Computer Science & Engineering

Ganga Institute of Technology and Management Kablana, Jhajjar, Haryana, India

[1]pk2235@gmail.com; [2]puneet.gitam@gmail.com

Abstract— The appearance of mobile computing devices such as laptops, smart phones grew people started to expect to gain network connectivity. As a result several groups started working on means to accomplish this task. This led to wireless LANs being marketed by several companies however this proposed standard could be used in two ways, one with the presence of a base station and the other without the presence of a base station. In the latter case the computers would communicate to each other directly. This is called as an ad-hoc network. A further specified case of ad-hoc networks is when the nodes i.e., computers in this case are mobile. In these cases each node consists of a host and a router on the same device. This means that the nodes form a network without the use of an external routing device.

Keywords— Company, Network, Connectivity, Nodes, Security

I.INTRODUCTION

As the appearance of mobile computing devices such as laptops, smart phones grew people started to expect to gain network connectivity. As a result several groups started working on means to accomplish this task. This led to wireless LANs being marketed by several companies. However this proposed standard could be used in two ways, one with the presence of a base station and the other without the presence of a base station. In the latter case the computers would companies to each other directly. This is called as an ad-hoc network. A further specified case of ad-hoc networks is when the nodes i.e., computers in this case are mobile. In these cases each node consists of a host and a router on the same device. This means that the nodes form a network without the use of an external routing device. When a number of such nodes happen to be near to each other and form networks, and is called as ad-hoc network or Mobile ad hoc network (MANET). As we are aware now that MANETs do not have a fixed topology, thus every single node in the network acts as a host as well as a packet forwarding device i.e., a router. Further the nodes in a MANET can move in any direction and are allowed leave the network at any point of time.

II. LITERATURE REVIEW

Nilotpal Chakra borty(2013) "intrusion detection system and intrusion prevention system: a comparative study

Intrusions in computing environment are a very common undesired malicious activity that is going on since the inception of computing resources. A number of security measures have taken place for the last three decades, but as Technology has grown up, so as the security threats.

Besant's Kumar(2013) "Intrusion Detection System- Types and Prevention" [2]

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates ace potable use policies. This article aims at providing a general presentation of the techniques and types of the intrusion detection and prevention systems, an in-depth description of the evaluation, comparison and classification features of the IDS and the IPS.Many IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control.

Dr. S.Vijayarani (2015) "intrusion detection system –

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

Nilotpal Chakra borty(2013) "**intrusion detection system and intrusion prevention system: a comparative study"[1]** Intrusions in computing environment are a very common undesired malicious activity that is going on since the inception of computing resources. A number of security measures have taken place for the last three decades, but as Technology has grown up, so as the security threats. With the whole world depending on computers, being directly or indirectly, it is a very important issue to prevent the malicious activities and threats that can hamper the computing infrastructures.

III. DESIGN METHODOLOGY

Socket Programming

The endpoint in an inter process communication is called a socket, or a network socket for disambiguation. Since most communication between computers is based on the Internet Protocol, an almost equivalent term is Internet socket .

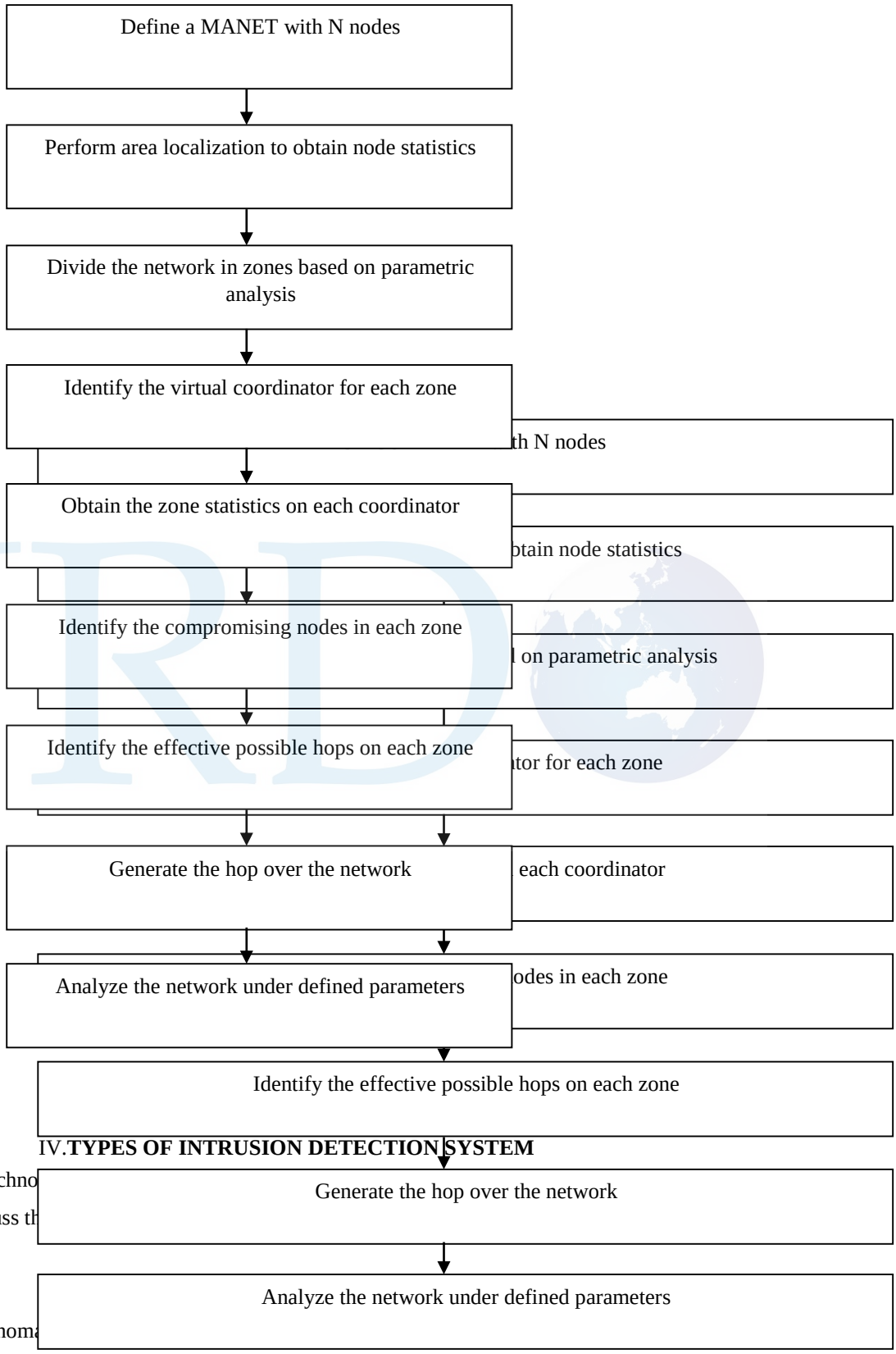
Client server Model

It is possible for two network applications to begin simultaneously, but it is impractical to require it. Therefore, it makes sense to design communicating network applications to perform complementary network operations in sequence, rather than simultaneously. The server executes first and waits to receive; the client executes second and sends the first network packet to the server.

FRAME 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



IV. TYPES OF INTRUSION DETECTION SYSTEM

There are many types of IDS techno

Here in this document we discuss th

1. Network Based IDS
2. Wireless IDS
3. Network Behaviour Anoma

4. Host Based IDS

1. NETWORK BASED IDS

Network based IDS (NIDS) monitors' network traffic for a particular network segment and analyses the network and application protocol activity to identify suspicious activity. It is most commonly deployed at a boundary between networks such as in routers, firewalls, virtual private networks etc.

2. WIRELESS IDS

A wireless local area network (WLAN) IDS is similar to NIDS in that it can analyse network traffic. However, it will also analyse wireless-specific traffic, including scanning for external users trying to connect to access points (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks increasingly support wireless technologies at various points of a topology, WLAN IDS will play larger roles in security.

3. NETWORK BEHAVIOR ANOMALY DETECTION

Network behavior anomaly detection (NBAD) views traffic on network segments to determine if anomalies exist in the amount or type of traffic. Segments that usually see very little traffic or segments that see only a particular type of traffic may transform the amount or type of traffic if an unwanted event occurs. NBAD requires several sensors to create a good snapshot of a network and requires benchmarking and base lining to determine the nominal amount of a segment's traffic

4. HOST BASED IDS

In Host-based IDS (HIDS) technology, software agents are installed on each of the computer hosts of the network to monitor the events occurring within that host only. HIDS analyze network traffic and system-specific settings such as software calls, local security policy, local log audits, and more. It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. HIDS are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

V.PROPOSED WORK

In this research we focus on Enhancement working of Intrusion detection System. In order to detect the Intrusion we need to trace the packets and routes of data transmission. Here we would perform all these using socket programming. To do this we would perform following tasks:

Step 1 Establish a data transmission mechanism to send and receive packets using socket programming in java. Here we would use port number more that 1024 because these port are free to use.

Step 1 To perform data transmission .from client to server and server to client.

Step 2 To trace the network route and detect the anomalies during data transmission

Step 3 To verify the data packets during transmission and removal of anomalies.

Step 4 To makes the data secure using encryption mechanism.

Step 5 Create a database to confirm the authenticity of packets and detect and remove all those packets that are not present in database.

VI.CONCLUSIONS

Identifying trusted data sources & marking data coming from these sources as trusted, Using dynamic tainting to track trusted data at runtime, & Allowing only trusted data to form semantically relevant parts of queries such as SQL keywords & operators. Unlike previous approaches based on dynamic tainting, our technique is based on positive tainting, which explicitly

identifies trusted (rather than untrusted) data in a program. This way, we eliminate problem of false negatives that might result from incomplete identification of all untrusted data sources. False positives, although possible in some cases, could typically be easily eliminated during testing. 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.

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 B.Santos Kumar(2013) "Intrusion Detection System- Types and Prevention" International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013*
2. *Dr. S.Vijayarani (2015) "INTRUSION DETECTION SYSTEM – A STUDY" International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015*
3. *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.*
4. *T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," in Wireless Network Security, pp. 159–180, Springer, 2007.*
5. *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.*
6. *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.*
7. *A. Nadeem and M. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," 2012.*
8. *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.*
9. *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.*
10. *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.*
11. *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.*
12. *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.*
13. *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.*