International Journal of Latest Trends in Engineering and Technology
Vol.(7)Issue(3), pp. 063-068
DOI: http://dx.doi.org/10.21172/1.73.509
e-ISSN:2278-621X

Detecting and Tracking Intruders in Mesh based Networks

Palamdeep Kaur[1] and Parminder Singh[2]

Abstract- There are number of threats that break the security of the network and branches all over network. Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations. An intrusion detection system (IDS) is one that permits to obtain information from different sources of the system where it has been implanted to alert of a possible intrusion in our network. The system will be informed about how the attack is being carried out or who is trying to break into the system. Sometimes it only can inform about the presence of an attack and nothing else. The proposed approach will be identify misbehaving nodes and makes them unable to interfere with routing. Thus, the routing protocol should be designed to be immune to malicious nodes.

Keywords- Mobile Ad hoc networks, Intrusion detection system(IDS), Nodes, Routing protocol.

I. INTRODUCTION

An intrusion is a type of attack on information assets in which the insitigator attempts to gain entry into a system or disrupt the normal operations of a system. Intrusion Detecting components analyse system and user operations in computer and network systems in search of activity considered undesirable from a security perpective. Data sources for anomaly-based intrusion detection may include audit trails produced by an operating system, or network traffic flowing between systems, or application logs, or data collected from system probes. The Mobile Ad-hoc Network (MANET) is the network that is easy to use and and seems attractive. The open and dynamic operational environment of MANET makes it vulnerable to various network attacks. Mobile Ad hoc networks or MANETs are the type of networks that is category of wireless network which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure. As shown in Figure.1, there are no base stations and every node must co-operate in forwarding packets in the network.

[1] *Department of Information and Technology Chandigarh Engineering College,Landran,Punjab,India*
[2] *Department of Information and Technology Chandigarh Engineering College,Landran,Punjab,India*

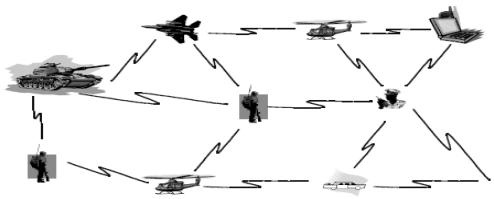

Figure 1: Overview of Mobile Ad-hoc Network

Design Issues of MANETs

The following design issues must be considered before designing a routing protocol for

MANETs [1]:

1. The network topology keeps changes with time due to the movement of the nodes by this the links between the nodes are breaks in the MANET. Therefore, the ordinary routing is only efficient for the static network not for the wired network. This the Dynamic Topology.
2. On the wireless network the information must be broadcast to all the neighboring nodes by the nodes in the MANET and by this channel itself is prone that occurs the several errors such as attenuation, multipath, etc. That is the Error prone broadcast channel. Thus the routing protocol itself must be designed taking into consideration these issues.
3. Many problems can occurs in the network due to use of contention based protocols such as CSMA/CD. The nodes send the data frames when the nodes are in out of range and then these nodes sends the data frames to node which is in the range so the collision of data frames occurs that are hidden terminal problem. So this can be resolved by the RTS/CTS handshake.
4. The exposed terminal problem is the problem in which the sender node is in range but the receiver node is out of range. So this can be resolved by routing protocol must reduce the number of broadcast packets to minimize the collision.
5. The low bandwidth nodes in the network as the traditional wired network are the high bandwidth. So when routing protocol is designing for MANET then the utilization of bandwidth by the routing protocol must be minimized in the network that is the Bandwidth constraint.
6. Nodes such as PDA, laptops, etc that are straightest power requirement in MANET and some of the devices have the limited power. Thus the routing protocols must be efficient in power conservation.

II. RELATED WORK

Authorname	Contribution	Gap
Mohiuddin Ahmed, et. al. (2016)	Intrusion Detection is the process of monitoring the events occurring in a network and analyze them.	Overhead has increased in the proposed study and difficult to calculate the log time events.
Rup Kumar Deka ,et. al. (2015)	Intrusion Detection makes the baseline of the normal usage pattern.	This paper did not adopt distribution technique hence it failed to detect the IDS threshold value.
Salim EL KHEDIRI et al. (2014	worked on performance of three types of Mobile Ad-hoc network routing protocols.	The problem has sorted in DSR, AODV and DSDV protocols and improve the QoS issues but energy problem is their and consume more energy in many cases.
Hung-Jen Liao, et. al. (2013)	Intrusion prevention is the process of performing ID and stop detected possible incidents	This paper levels has defined and difficult to model DoS attack other than IPS attack. Operating system kernel problem might be their in some conditions.

III. EXISTING PROBLEM

While the use of wireless links renders a mesh network susceptible to attacks, the physical exposure of the nodes allows an adversary to capture, clone or tamper with these devices.

The two attacks are Denial of services (DOS) and Distributed Denial of services (DDOS), but the most harmful attack is the Rushing attack which is the part of Denial of service.

A rushing attack is an effective IDS Network based attack against on-demand routing protocols.

To limit the overhead of Route Request (RREQ) flood, each node typically forwards only the first RREQ originating from any route any route discovery. Utilizing this property, an attacker that forwards RREQs more quickly than legitimate nodes can do so, can increase the probability that routes including the attacker will be discovered rather than other valid routes.

The proposed algorithm will be identify misbehaving nodes and makes them unable to interfere with routing.

Alternatively, the routing protocol should be designed to be immune to malicious nodes.

IV. PLANNING OF WORK

- The base station and nodes maintain information regarding their view of the network structure.

- The node structure contains a list of all paths to each node, each node's hop count from the base station, ID, and individual key.
- The group structure maintains information about all groups in the network in a linked list of group elements.
- A group element contains information about the group including a listing of all nodes IDs, the distance from the base station to the group (called the level), and methods used for group membership authentication.

V. RESULTS AND DISCUSSIONS

A. *THROUGHPUT OF NETWORK-*

The throughput of the network defined the total number of packet sent from the sender side with ratio of total number of received packets. The output ratio converted into bytes and the result represented in bits/seconds.

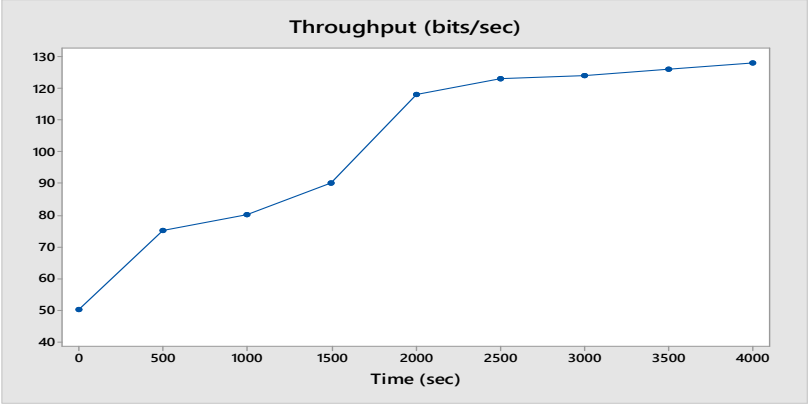

Figure 2: Throughput of Network with ICMP attack

B. *DATA DROPPED-*

The data dropped represents the total number of packets dropped on the mobile network either from communicating nodes or base station.

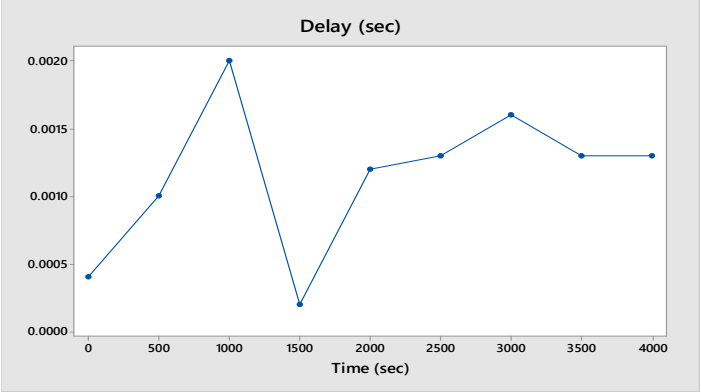

Figure 3: Data Dropped with attack

C. LOAD AND NETWORK DELAY-

The analyzed the load distribution in the network in order to get more information about the working behavior of IDS.

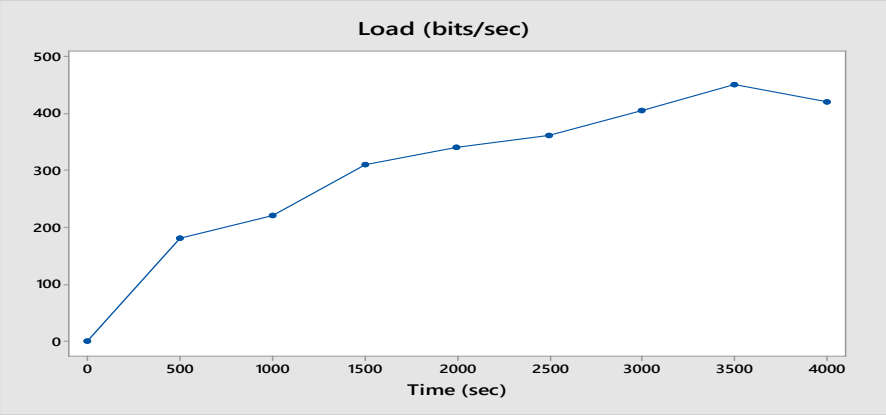

Figure 4: Network Load with attack

VI. CONCLUSION

In this paper proposed technique was introduced to increasing the security of the network. The main impact of this paper that increasing the security level that overhead the authentication, authorization, and routing delay. Rushing attack access the useful information from the network. The attack scenario explores the rushing attack from the selfish node, accesses important information from the neighboring machine, or it creates virtual path to the victim node. This attack degrades the performances of the network with increase of network load and delay. The time improve the performances of the attack scenario after evaluation in the current scenario. In this paper the proposed technique is to created new path to authenticate the client on the same scenario by confirmation of MAC based address.

REFERENCES

[1] Mohiuddin Ahmed, AbdunNaser Mahmood, Jiankun Hu.,"A survey of network anomaly detection techniques",*Journal of Network and Computer Applications,2016*, pp. 19-31.

[2] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, Kuang-Yuan Tung,"Intrusion detection system: A comprehensive review,*Journal of Network and Computer Applications",2013*, pp.16-24.

[3] Whitman, M.E. and Mattord, H.J. ,"Principles of Information Security, Thomson CourseTechnology, Boston, MA",2005.

[4] Martin, C. (2009), "What is IPS and how intrusion prevention system works", available at: www.aboutonlinetips.com/what-is-ips-and-how-intrusion-prevention-system-works/ (accessed 10 October 2009).

[5] Rup Kumar Deka, KausthavPratimKalita, D.K. Bhattacharya, Jugal K. Kalita,"Network defense:Approaches, methods and techniques", Journal of Network and Computer Applications,2015.

[6] Ahmed Patel, Samaher Al-Janabi, Ibrahim Al-Shourbaji, Jens Myrup Pedersen,"A NovelMethodology towards a Trusted Environment in Mashup Web Applications. Computers & Security",2015.

[7] Shruti, Umang, Prof.B.V. R. Reddy, Prof. M.N. Hoda, "Analytical Study of Existing Methodologies of IDS for False Alarm Rate - A Survey and Taxonomy", IJEATE, 2012, pp.393-399.

[8] C.J. Tucker S.M. Furnell B.V. Ghita P.J. Brooke,"A new taxonomy for comparing intrusion detectionsystems", Internet Research, Vol. 17 Iss 1, 2007, pp. 88 - 98

[9] A.S. Sodiya H.O.D. Longe A.T. Akinwale,"Maintaining privacy in anomaly-based intrusion detectionsystems", Information Management & Computer Security, Vol. 13, Iss 1,2005, pp. 72 - 80

[10] A.S. Sodiya H.O.D. Longe A.T. Akinwale,"Maintaining privacy in anomaly-based intrusion detectionsystems", Information Management & Computer Security, Vol. 13, Iss 1,2005, pp. 72 – 80

[11] Rod Hart Darren Morgan Hai Tran, "An introduction to automated intrusion detection approaches", InformationManagement & Computer Security, Vol. 7, Iss 2,1999, pp. 76 - 82

[12] DjamelDjenouri, NadjibBadache, "MANET: Selfish Behavior on Packet Forwarding" Encyclopedia of Wireless and Mobile Communications, 2008, pp.576-587.

[13] Muhammad Mizanur Rahman," Performance analysis of Leader Election Algorithms in Mobile Ad hoc Networks", IJCSNS, 2008, pp 257-263.

[14] I.Shanthi, D. SornaShanthi, "Detection of false alarm in handling of selfish nodes in MANET with congestion control", IJCSI, 2013, pp.449-457.

[15] Chun-Ta Li,Chou-Chen Yang,"A secure routing protocol with node selfishness resistance in MANETs",International journal of Mobile Communications,2012,pp.103-118.

[16] Naveen Kumar Gupta, Ashish Kumar Sharma, Abhishek Gupta,"Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS) IJRREST, 2012,pp 31-34.

[17] Shruti, Umang, Prof.B.V. R. Reddy, M.N. Hoda, "Analytical Study of Existing Methodologies of IDS for False Alarm Rate - A Survey and Taxonomy", IJEATE, 2012, pp.393-399.