IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

Intrusion Detection System for Mobile Ad - Hoc Network Using Cluster-Based Approach

Nisha Dang[1], Pooja Mittal[2]

[1]M.tech Student, Department of Computer Science and Applications,
M. D. University, Rohtak-124001, Haryana, India
nishadang21@rediffmail.com

[2]Assistant Professor, Department of Computer Science and Applications,
M. D. University, Rohtak-124001, Haryana, India

Abstract

Today Mobile Ad-hoc Networks have wide spread use in normal as well as mission critical applications. Mobile ad hoc networks are more likely to be attacked due to lack of infrastructure and no central management. To secure Manets many traditional security solutions like encryption are used but not find to be promising. Intrusion detection system is one of the technologies that provide some good security solutions. IDS provide monitoring and auditing capabilities to detect any abnormality in security of the system. IDS can be used with clustering algorithms to protect entire cluster from malicious code. Existing clustering algorithms have a drawback of consuming more power and they are associated with routes. The route establishment and route renewal affects the clusters and as a consequence, the processing and traffic overhead increases due to instability of clusters. The ad hoc networks are battery and power constraint, and therefore IDS cannot be run on all the nodes. A trusted monitoring node can be deployed to detect and respond against intrusions in time. The proposed simplified clustering scheme has been used to detect intrusions, resulting in high detection rates and low processing and memory overhead irrespective of the routes, connections, traffic types and mobility of nodes in the network.

Keywords: *IDS, MANET, Detection Systems.*

Introduction

Mobile ad hoc networks have gain popularity in a very short period of time due to instant and fast network connections as and when required. A Mobile Ad hoc Network (MANET) is a collection of mobile nodes that are dynamically and arbitrarily located and the interconnections between them are capable of changing on a continual basis. In MANET each node acts as a host as well as a router for directing a packet to its destination route.

Mobile ad hoc networks or Manets find their use in many mission critical applications such as military operations and rescue missions as well as in mobile conferencing and variety of other applications.

MANET have some limitations such as changing network topology, limited transmission range, limited processing and power sources, low availability of bandwidth due to wireless environment and consumption of higher control packets for establishing and maintaining the routes.

Due to the wireless nature and distributed environment Manets are more vulnerable to various types of attacks. They have vulnerabilities like any other network of eavesdropping, spoofing, denial of service, signal jamming etc. One of the major problem in Manets is each node is equally trusted so any malicious node can easily become part of network and fabricate or simply drop the packets. Therefore, security becomes a prime concern to provide a secure communication in Manets.

Intrusion detection system can be used to protect these wireless multi-hop networks to protect them against a number of attacks by providing auditing and monitoring capabilities. This Intrusion Detection System is used to detect Intrusion, identify the malicious nodes and isolate them from the rest of the network. Further the presence of a detection system will discourage malicious nodes from attempting intrusion in future. But the normal IDS is not well suited for these networks due to mobility, power and processing constraints. Also heavy control files cannot be run on each node. Therefore, a scalable and fault tolerant IDS is required to protect these wireless networks against attacks.

Intrusion Detection System

IDS is a combination of hardware and software that checks each and every activity of user to find any abnormal or malicious activity. In other words, it

IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

compares the normal activities with intruders' activity. So an IDS is a professional guard system that observes patterns of activities in user accounts and alert a system administrator if anything unusual (intrusion) is detected.IDS system while detecting any unusual activity, take steps to prevent such activities to effect computer security such as confidentiality, integrity, authentication, non-repudiation and availability.

Intrusion detection System Classification

Intrusion detection can be classified based on audit data as either host-based or network-based. A network- based IDS (NIDS) checks the network traffic for any abnormality or malicious code. A host-based IDS (HIDS) checks the system for any abnormal action by using operating system functions or application programs. Focusing mainly on network traffic data and computer audit data, there are two general approaches to detecting intrusions: misuse based intrusion detection and anomaly based intrusion detection. They are complementary to each other for intrusion detection.

Anomaly detection systems

Anomaly detection system keeps a record of the normal activities of the user. As user performs any activity it is compared from the activity log. If any abnormality is found the system generates the alarm or an alert message to inform the system administrator about the intruding activity so that necessary actions can be taken. Anomaly detection system can use different techniques for detecting intruders' activities such as statistics count, neural networks etc.

Misuse Detection system

The misuse detection system keeps the record of the well known attacks or signatures of existing attacks. If any activity matches with one of the attacks type then necessary actions are taken so that security can be prevented. But this IDS have a drawback that any new type of attack can not be identified. Misuse Detection System can use several approaches such as expert systems, pattern recognition, state transition analysis etc.

IDS in Manets

Intrusion detection in Manets is a tough job as nodes in Manets change dynamically. So a malicious node can easily become a part of the network and can send false routing information, drop or modify data or control packets. There is no clear definition of normal and malicious activities for mobile ad hoc networks. Therefore, the Intrusion Detection architecture for Manets should be simple and effective to provide security against different type of attacks. Many Intrusion detection systems have been proposed for Manets such as Standalone intrusion detection system, Distributed intrusion detection system, Hierarchical intrusion detection system.

The efficient approach to prevent against intrusion in Manets is to detect the intrusion cooperatively, rather than each mobile node performing full analysis of traffic passing through it and to work with cooperation each node must trust other node in the network so that they don't have to check all the data thus saving a lot of processing and memory overhead. The clustering in MANETS can be used as an advantage for the purpose of intrusion detection, by separating tasks for the head and member nodes.

Therefore, a low-overhead clustering algorithm is proposed for the benefit of detecting intrusion rather than efficient routing. The proposed simplified clustering scheme and its architecture have been used to detect intrusions under various attacks and it results in high detection rates and low processing and memory overhead.

Related work

Security is a prime concern in Mobile ad hoc networks and many researchers have given their important views and research works regarding it.

Zhang et al. had proposed an intrusion detection system which was based on modular approach. In this system each node independently detects the intrusion using some detection modules. The node can take cooperation of other nodes if it is not able to decide about the intrusion. In this solution each node have to run many modules so it requires more processing and memory overhead.

Li et al. had given a new direction to intrusion detection. He proposed the use of mobile agents that detects intrusion and generates response within a network. These mobile agents work collaboratively at all nodes and thus increasing processing and memory usage on each node.

Albers et al. also proposed an IDS by using mobile agents. Albers proposed a Local Intrusion Detection System (LIDS) that is implemented on every local node for detection of malicious activity. This LIDS can be used for global intrusion detection by communicating with other LIDS. These intrusion detection systems communicate two types of data: security data and intrusion alerts.

Kachirski and Guha proposed a multi-sensor

IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

intrusion detection system. This IDS also uses mobile agent technology. This system uses three main mobile agents with different functionalities, i.e.: monitoring, decision-making and initiating a response.

A cooperative intrusion detection system for mobile ad hoc network security was proposed by Yi-an et al. It deals with cluster-based intrusion detection and also reduces the processing and memory overhead. The cluster formation and cluster head selection for cooperative intrusion detection is done through clique computation and cluster head computation protocols. But it introduces the overhead in Clique computation and exchange of Hello messages for checking the existence of member nodes in clusters.

Proposed Cluster Based Approach

The proposed clustering algorithm can run on top of any routing protocol and can monitor the intrusions constantly irrespective of the routes. This proposed simplified clustering scheme and its architecture has been used to detect intrusions, resulting in high detection rates and low processing and memory overhead irrespective of the routes, connections, traffic types and mobility of nodes in the network. The proposed works involves

- Cluster formation
- Intrusion Detection Architecture

The proposed generic clustering algorithm performs elections irrespective of the routes, and has its own HELLO messages. It does not degrade network performance by re-establishing the routes, which is required in other clustering algorithms when the cluster-head is changed. The overhead, as compared to other clustering algorithms, is minimal since we keep neighbor information only at the head node and the amount of broadcast HELLO messages is also reduced.

Cluster Formation

The clusters are formed to divide the network into manageable entities for efficient monitoring and low processing in the network. The clustering schemes result in a special type of node, called the Head Node (HD) to monitor traffic within its cluster. It not only manages its own cluster, but also communicates with other clusters for cooperative detection and response. It maintains information of every member node and neighbor clusters, which is useful for network-wide communication. The cluster management responsibility is rotated among the capable members of the cluster for load balancing and fault tolerance and must be fair and secure. This can be achieved by conducting regular elections.

A node in ad-hoc network can be in one of the 4 possible states:

- UNDECIDED (UD)
- HEAD (HD)
- MEMBER (MB)
- GATEWAY (GW)

Initially, every node is in UD state. It starts election and may become HD node if it does not have link to any HD node, otherwise it goes to MB State if it finds any HD node in the neighbor. When a MB node looses its head, it returns back to UD state. If the MB node finds another HD node among its neighbor (due to mobility or election process), it becomes GW. Both the MB or GW nodes can move to HD state after Election. Simultaneously, HD node upon failing in the election process becomes MB or GW. The GW node upon loosing its HD node(s) except one also goes back to MB State.

Intrusion Detection Architecture

Intrusion detection architecture in clusters mainly consists of four modules to detect the intrusion. That are:

- Data Collection / Logging Module
- Intrusion Information Module
- Intrusion Detection Module
- Alert Module

Data Logging/Collection Module

The traffic passing through the head node is monitored by the head node and necessary information is logged in a database. This logged information is used later for detecting the abnormal or intruding activity. Head node performs the traffic analysis and sends the packets to the member nodes which perform the packet analysis for malicious code. Thus reducing load at a single node.

Intrusion Information Module

Along with the database maintained at the head node each other node in the cluster maintains a database for intrusion information that is it stores the record of intruding activities or processes. This database is used for interpretation of intrusion in future. The abnormal behavior detected by the node must be dealt in time and recorded in the database. So that the database always remain updated for new type of intrusions.

IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

Intrusion Detection Module

Intrusions can occur at any of the layer of TCP/IP protocol stack. So, it is very crucial to detect the intrusions at all layers. This module describes the detection mechanism at all the layers. At the application layer, the intrusion is monitored by user authorization & login attempts. The established sessions, protocols usage, connection time, etc can be handled at the transport layer. The routing table management, routes verification is handled by network layer. At the data link layer, the transmitting nodes, CSMA/CD, used channels, etc are of important concern to be handled. The concerns at the physical layer are that with direct physical access to the system.
The cluster-head logs all the data transfer activities within its radio range. This log can be used for the traffic analysis from a certain source node. Therefore, the log-based detection is useful for the partial analysis at the cluster-head.

Alert Module

This module shows the response mechanisms. The cluster member node takes necessary security prevention steps and informs the cluster-head about the response. The cluster-head node informs other nodes about the intrusion either when a member node informs it about a found intrusion or when it receives a response from neighbor cluster-heads. The response may be local to the cluster or global to the whole network.
The cluster-head generates a cluster-based response to the cluster in any of the 3 cases: a member node has informed about an intrusion, after log-based detection, or after getting response from adjacent cluster. The cluster-head can also generate a network-wide response. In the first 2 cases of cluster-based response, network-wide response is optional, whereas in the third case, it is mandatory to inform the whole network about the intrusion.

Performance Evaluation

Hardware and Software Requirements

Hardware

- Color Monitor
- Intel Pentium 4 processor 2.8Ghz.
- 512 MB RAM.
- 40GB hard disk.
- 845G Motherboard

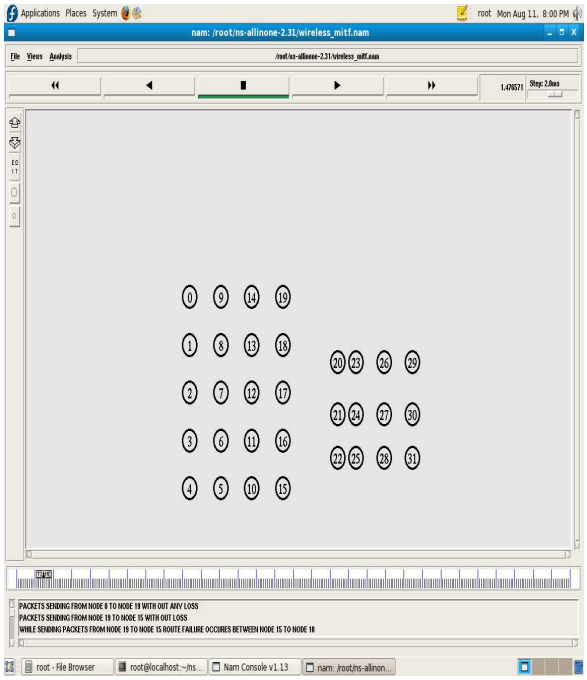
Software

- REDHAT 9 LINUX.
- NS-2 (NETWORK SIMULATOR-2) TOOL.

Implementation Parameters for MANETs

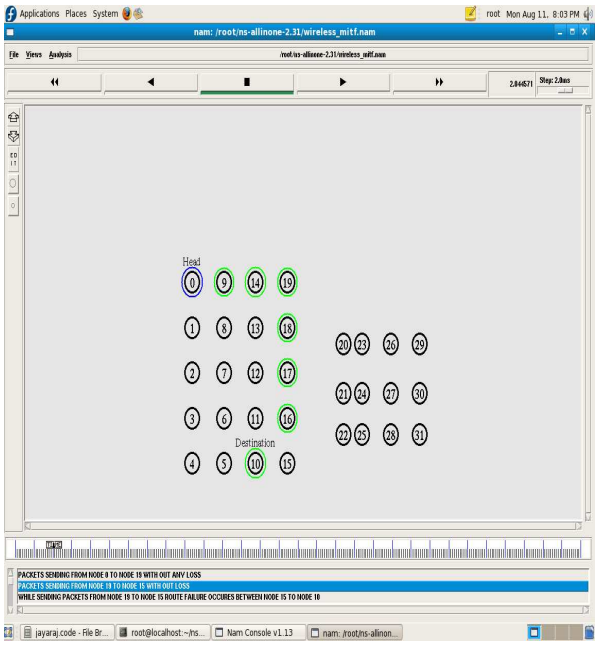
Channel	Wireless
Propagation	Two ray
MAC	802.11
Queue	Drop tail/ pri queue
Antenna	Omni directional
Dimension(X,Y)	1000,1000
Routing Protocol	AODV
Simulation Time	100s
Connection Pattern	CBR

Simulation and Results

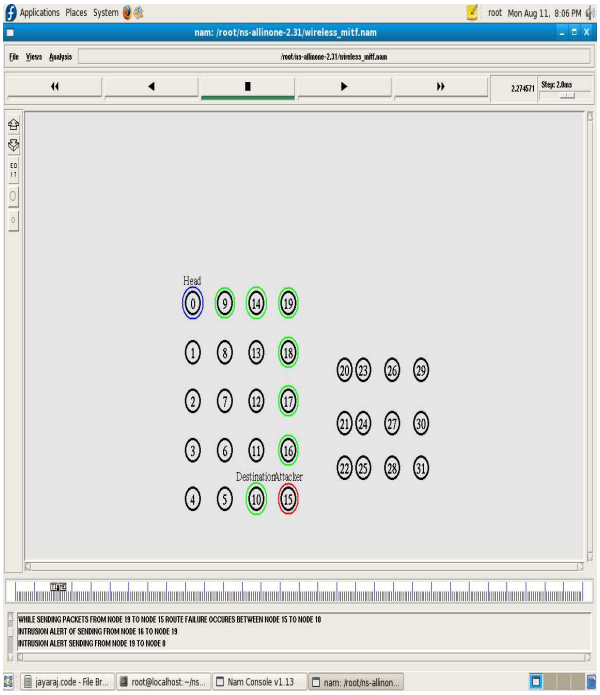


SS 1: Formation of Cluster from the given nodes

IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com



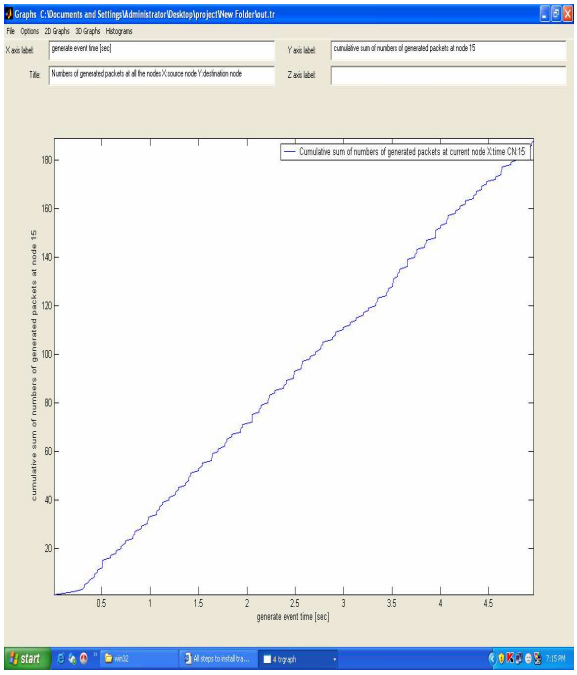
SS 2: HEAD NODE SELECTION FROM THE CLUSTER



SS 3: Intrusion detection in the cluster

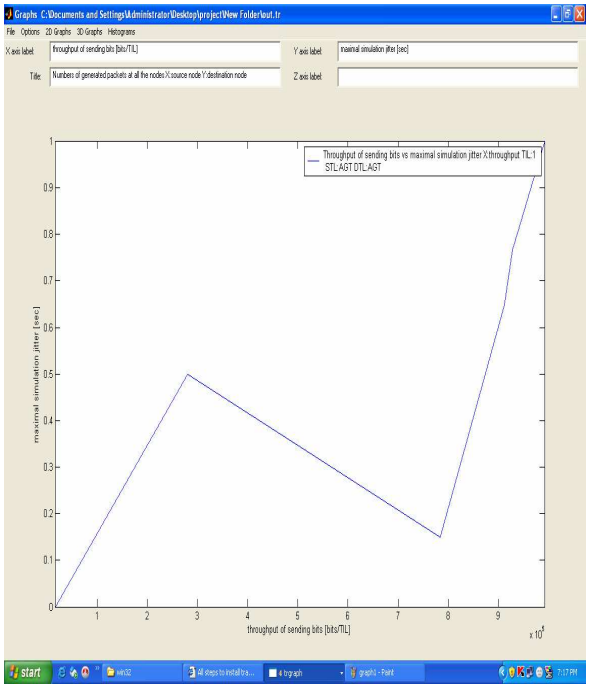
Experimental Results

Inputs that are given are the node id, number of mobile nodes and their radio range and link description about the nodes. The output is that detection of the malicious nodes and the simulation of graphs giving the degradation of the performance based on packet delivery ratio, end to end delay, throughput and delay jitter.

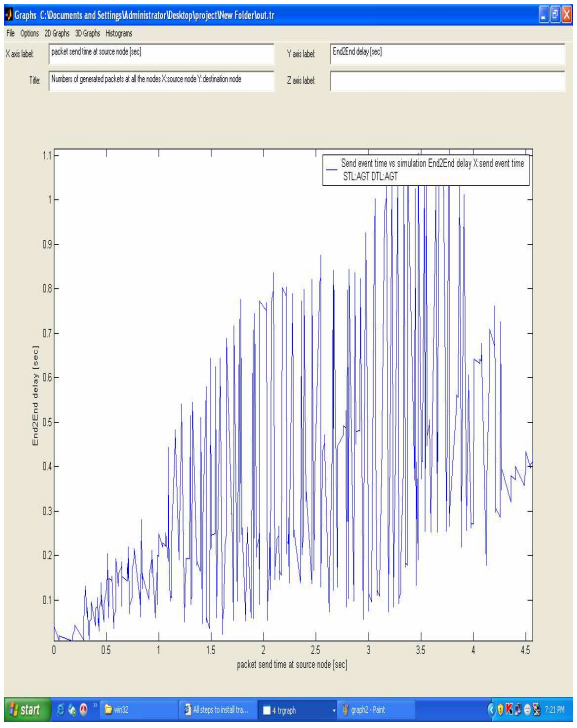


SS 4: Performance of packet delivered ratio

IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com



SS 5: PERFORMANCE OF THROUGHPUT



SS 6: PERFORMANCE OF END TO END DELAY

Conclusions and future Work

In this paper we have proposed a cluster based intrusion detection system and compared it with existing intrusion detection systems. We have found that this IDS is useful in clusters as it reduces processing and memory overhead and load of data transfer on network for detected intrusion or for detection of intrusion.

In future work we are trying to make this algorithm more effective and less time consuming. Also memory and processing overhead should be minimum. Cluster formation and division of head and member nodes responsibilities should be instantaneous. All these processes are our target to be modified.

References

[1] Kashan Samad, Ejaz Ahmed, Waqar Mehmood: MultiLayer Cluster-based Intrusion Detection Architecture for Mobile Ad Hoc Networks using Mobile Agents , Hi Optical Networks and Enabling Technology (HONET), Islamabad, Pakistan, Dec 28-31, 2004.

[2] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis and Y. Yesha "Threshold-based intrusion detection in ad hoc networks and secure AODV," Ad Hoc Networks, Vol. 6, Issue No. 4, pp. 578-599. June 2008.

[3] Yi-an Huang, Wenke Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", inProceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN), Fairfax, Virginia,October 31, 2003.

[4] Yu Liuy, Yang Liy, Hong Many, "MAC Layer Anomaly Detection in Ad Hoc Networks", 6th IEEE Information Assurance Workshop, USA, 15-17 June 2005.

[5] Kashan Samad, Ejaz Ahmed, Waqar Mahmood, "Simplified Clustering Scheme for Intrusion Detection in Mobile Ad Hoc Networks", 13th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, September 15-17, 2005.

[6] S.Bansal, M.Baker, "Observation based cooperation enforcement in ad hoc networks," Research Report cs. NI/0307012, StanfordUniversity.

[7] Ningrinla Marchang, Raja Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks," Ad Hoc Networks, Vol. 6, Issue No. 4, pp. 508-523 June 2008

IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

[8] Yongguang Zhang, Wenke Lee, "Intrusion Detection in Wireless Ad-Hoc Networks" , Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, MobiCom 2000, Boston, Massachusetts, Aug 6 11, 2000, pp 275-283.

[9] Chunsheng Li, Qingfeng Song, Chengqi Zhang: "MA-IDS Architecture for Distributed Intrusion Detection using Mobile Agents", Proceedings of the 2nd International Conference on Information Technology for Application (ICITA), 2004.

[10] Yi-an Huang, Wenke Lee, "A Cooperative Intrusion Detection System for AdHoc Networks", in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN), Fairfax, Virginia, October 31, 2003.

[11] Mingliang Jiang, Jinyang Li, Y.C. Tay: "Cluster Based Routing Protocol (CBRP)", Internet Draft, Jul, 1999.

[12] Yunjung Yi, Mario Gerla, Taek-Jin Kwon: Efficient Flooding in Ad-Hoc Networks using On Demand (passive) Cluster Formation , Proceedings of Mobihoc, Jun 2003.