Hybrid Approach: Detection of Intrusion in Manet

Rubana Tarannum
Research Scholar
S.I.R.T.,Bhopal

Megha Lamble
Asst.Professor
S.I.R.T.,Bhopal

ABSTRACT
As the progression of networks is continues, Mobile ad hoc network (MANET) has become as a new frontier of technology to give anywhere, anytime communication. Because of the features like unreliability of wireless links between nodes, dynamic topology, limited battery power, lack of centralized control and others, the mobile ad hoc networks are more vulnerable to suffer from the malicious behaviors than the traditional wired networks. The topology of an ad hoc network is defined by the geographical positions and the transmission ranges of the nodes. The Prevention methods like , Firewalls , authentication and cryptography techniques alone are not able to provide the security to these types of networks. Therefore, efficient intrusion detection must be deployed to facilitate the identification and isolation of attacks. In this paper we have discussed an Intrusion detection system for Mobile Ad-hoc Networks using a hybrid approach which consists of local as well as global detection using reactive and proactive protocols.

Keywords
Mobile Ad-hoc Network, Security, attacks, Intrusion Detection, local ,global, reactive, proactive, hybrid.

1.INTRODUCTION
Wireless has opened a new and exciting world for many of us. Its technology is advancing and changing every day and its popularity is increasing. The biggest concern with wireless, however, has been security. mobile ad hoc network (MANET) is a collection of mobile nodes that are capable of communicating with each other, establishing and maintaining connections as needed. In ad hoc networks, there is no established infrastructure or centralized administration.[1]. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart rely on intermediate nodes to forward their messages. Each node can function both as a router as well as a host.[3]. The inherent features of mobile ad hoc networks make them more vulnerable to a wide variety of attacks by misbehaving nodes. These attacks can be a passive or active attacks. In active attacks, we mainly consider the internal attacks for network layer such as black hole attack, gray hole attack, worm hole attack, message tampering, routing attacks. A malicious node drops packets or generates additional packets solely to disrupt the network performance and prevent other nodes from accessing any network services (a denial of service attack) .[2]. Hence an intrusion detection system is required here to detect the attack in the system and provide a secure communication. A node that is accused of misbehavior is denied access to the network by its neighbors, which ignore any of its transmission attempts. Intrusion detection is a security mechanism which is used to identify those who are trying to break and misuse the system without authorization and those who have legitimate access to the system but misusing the privileges. The Intrusion detection System monitors the activities of the system, analyze the activities to determine that any of the activity is violating the security rules.[4]. Depending upon the technique used, the intrusion detection can be classified in 3 categories:

1. Misused or signature based IDS;
2. Anomaly based IDS;
3. Specification based IDS

In misuse based intrusion detection [4], also called signature based detection, a pre-written rule or pattern is used to match an attack. In anomaly detection, a normal profile of user is kept in the system and then the captured profile is compared. If IDS found any activity that deviated from the normal profile is detected as anomaly. In Specification based intrusion detection, some set of constraints are defined for correct operation of program and then operations are monitored against define constraints. A mismatch is reported as a attack.[4].In MANET number of nodes form a cluster. To find the attack within the cluster is called as local detection to detect the attack in another cluster is called as the global detection. In *ad hoc networks*, nodes do not start out familiar with the topology of their networks; instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them.

Pro-active (table-driven) routing: This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network example is DSDV-Destination-Sequenced Distance Vector routing protocol.

Reactive (on-demand) routing: This type of protocols finds a route on demand by flooding the network with Route Request packets. Example is AODV-Ad Hoc On Demand Vector.

Hybrid routing: This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice for one or the other method requires predetermination for typical cases.

2. EVOLUTION
Intrusion detection in MANET is addressed by various researchers and has been a major research area. In 1987 the dinning proposed a model of a real-time intrusion-detection expert system that can able to detect break-ins, penetrations, and other forms of computer abuse[5]. The model is based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns of system usage. In 2000, the S. Marti, T.J. Giuli, K. Lai and M. Proposed the "watchdog and pathrater" scheme that is used to detect & mitigate the effect of nodes that do not forward packets. In 2001 Knowledge-based intrusion detection systems was proposed by H.–Y. Chang, S.F. Wu and Y.F. Jou,

which accumulate knowledge about attacks, examine traffic and try to identify patterns indicating that a suspicious activity is occurring. This approach can be applied against known attack patterns only and the utilized knowledge base needs to be updated frequently [6]. In 2003, O. Kachirski and R. Guha proposed a sensor based approach to detect intrusion.[7]. In Aug 2004, D. Sterne, et al. Present a cooperative intrusion detection architecture[8] that facilitates accurate detection of MANET-specific and conventional attacks. In 2005, Ioanna Stamouli proposed RIDAN architecture which uses timed finite state machine to formally define attack against the AODV routing process. It uses a knowledge based methodology to detect the intrusion [9]. In [10] S.Bose, P.Yogesh and A.Kanan proposed a "Neural network approach for anomaly intrusion detection in ad hoc network using mobile agents". In Sept 2006 Xia Wang proposed end to end Wormhole detection method in wireless ah hoc networks [11]. In Oct 2006 Yu Liu, Cristina Comaniciu and Hong Man proposed a Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks [12]. In 2007, J Martin, R.Bhuvaneshwari, M.A. Bhagyaveni and S. Shanmugavel developed a secure routing approach called Resiliency Oriented Secure (ROS)which include the detection phase in routing to detect the malicious node. In June 2008 Ningrinla marching and Raja Datta proposed "collaborative technique for Intrusion detection in MANET"[13]. Pasquale Donadio, Antonio Cimmino and Giorgio Ventre proposed a Grid based Intrusion Detection System[14]. S.Madhavi and Dr. Tai Hoon Kim [15] developed an Mobile Intrusion Detection System for multi-hop ad-hoc wireless network. S Sen proposed a "grammatical evolution approach to intrusion detection on mobile ad hoc networks"[16]. They use artificial intelligence based learning technique to explore design space.

There are numerous techniques to detect the intrusion in MANET using only reactive approach or only using proactive approach .here we are proceeding with a hybrid approach to detect the intrusion in the MANET.

3. NEW ARCHITECTURE

The hybrid intrusion detection system is designed especially for the mobile ad-hoc network. We take into considerations, when designing our hybrid intrusion detection system, the characteristics of the wireless ad-hoc network and the problems that existing system face when being deployed in a wireless ad-hoc environment.

The dynamic and cooperative nature of the wireless ad-hoc network suggests that the intrusion detection system should be designed to be dynamic and cooperative as well. Each node should have its own intrusion detection module since it cannot rely on other nodes that may leave the network at anytime to help it perform intrusion detection. Wireless ad-hoc networks also do not have traffic concentration points that allows for intrusion detection at a centralized location and this further emphasize the need for each to have its own intrusion detection module.

Intrusion detection should first be performed locally on each node utilizing the partial, localized audit data since this is the most reliable source of audit data for a node. Each node can then perform cooperative intrusion detection when more information is required from other nodes to confirm the intrusion. For cooperative intrusion detection, the individual node is required to work with neighboring nodes to gather more audit data for intrusion detection. This suggests that there should be a secure communication channel between the nodes participating in the cooperative intrusion detection.

The last requirement for the hybrid system is that it should be scalable. As wireless ad-hoc networks are becoming more mainstream, such networks in the future may contain hundreds to thousands of nodes. A scalable system will ensure that intrusion detection still continue to function effectively and efficiently under a large number of nodes.

IDS of Hybrid structure separates the whole MANET into multiple IDS clusters; and the intrusion detection activity is executes by cluster head.

Hybrid structure of IDS system has excellent network extensibility and little network control overhead, which can realize distributed intrusion detection and is appropriate for network characteristics of the MANET. The host IDS can effectively distinguish and report information of attacks in the system.

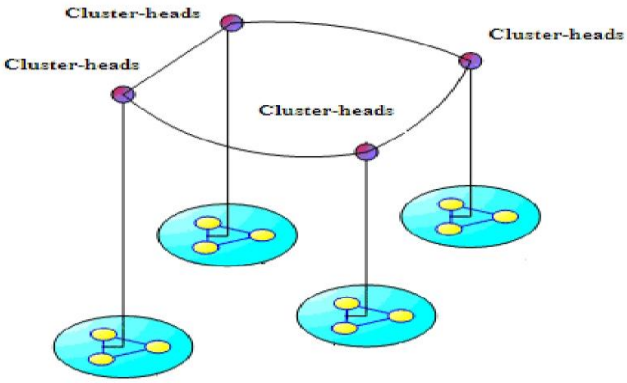

Figure 1 Hierarchical structure of IDS system

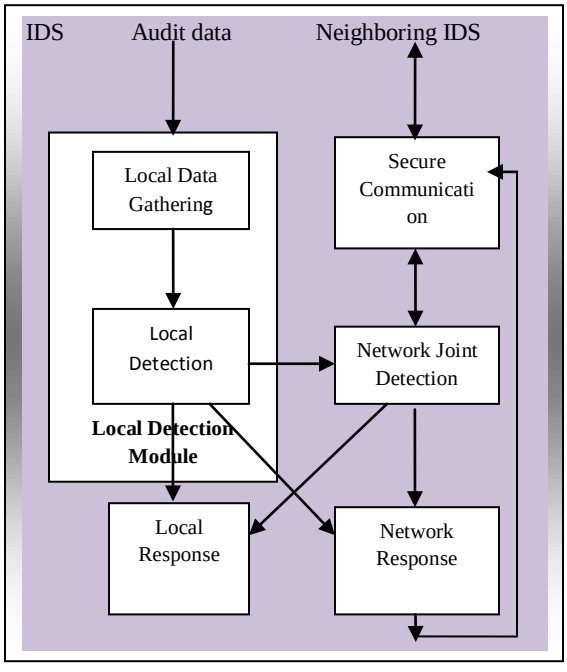

Figure 2 – IDS Using Hybrid Approach.

3.1Making cluster and choosing cluster head:

Clustering algorithm is mainly to build an interconnected cluster set that can cover the whole user node and can well support resource management and routing protocol. In analyzing the following text, the following conditions are always supposed true:

- Every node has unique ID; the node can obtain all neighbor nodes' ID by way of broadcast packet;
- The node can always exactly receive neighbor nodes' data pack;
- The network model meets momentary static model. [17].

3.2. Path Establishment and Forwarding Routing Table:

The AODV routing protocol is a reactive protocol designed for wireless ad hoc networks. When a source node needs a route to a destination, it initiates a route discovery process to locate the destination node. The source node floods the network with a route request packet (RREQ) requesting a route to be set up to the destination. On receiving an RREQ, intermediate nodes update their routing table with a reverse route to the source. All the receiving nodes that do not have a route to the destination broadcast the RREQ packet to their neighbors, with an incremented hop count. A route reply (RREP) is sent back to the source node when the RREQ query reaches either the destination itself or any other intermediate node that has a current route to the destination. As the RREP propagates to the source, the for-ward route to the destination is updated by the intermediate nodes receiving an RREP packet. When a link break occurs, route error (RERR) packets are propagated along the reverse path to the source, invalidating all broken entries in the routing tables of the intermediate nodes. AODV also uses periodic HELLO messages to maintain updated information about the connectivity of neighboring Audit data Neighboring nodes. Although the system uses Proactive approach. When ever the path is generated between the source and final destination they share their routing table.

3.3. Intrusion Detection:

The IDS runs on each node, executing data gathering and detection function. When it is found that local data is abnormal, or receiving abnormal report from neighbor nodes, cooperative detection among the nodes and total network intrusion detection is triggered Functions of each module are as the following:

1. Local data gathering: receiving data deliver by node in cluster, monitoring local data (such as obtaining message, monitoring update of route table and so on), classifying and computing the gathered data, etc.

2. Local detection: analyzing data, determining whether is intruded or not, triggering the joint detection application if necessary.

3. Local response: determining response strategy, broadcasting in the cluster. Possible response policies comprise reinitialized certificate information, reinitialized signal path, and blacklist operation, etc.

4. Network joint detection: when local cluster-head node can not determine intrusion, the joint detection request will be triggered to ask for other clusters to male joint detection. Trigger rule means all cluster-head nodes taking certain natural number as hop. The cluster head receiving joint detection request makes determination by analyzing data in the cluster of its own, and gives determination on possibility of attack. The cluster head launching joint detection request uses weighted algorithm to determine whether local intrusion is occurred based on results returned from other cluster-head nodes by principle of that the minority is subordinate to the majority.

5. Network response: for determined as intrusion-occurred node, making total network blacklist broadcasting.

Following Procedures are used simultaneously for the overall operation:

void ClusterAgent::routediscover();

void ClusterAgent::formcluster();

void ClusterAgent::select_clusterhead();

void ClusterAgent::send_keypair();

void ClusterAgent::receive_ack();

void ClusterAgent::complete_handshake();

void ClusterAgent::detect_malicious();

void ClusterAgent::ignore_malicious();

void ClusterAgent::create_schedule();

void ClusterAgent::split_up_packet(packet* p);

void ClusterAgent::SendscheduleToMembers();

void ClusterAgent::send_packets();

void ClusterAgent::recive_packets(packet* p);

void ClusterAgent::foward_send_RREQ_packets(packet* p);

voidClusterAgent::foward_send_RREP_packets(packet* p);

4. SIMULATION RESULTS

The proposed scheme has been implemented on network simulator *ns-2* [18] to evaluate its performance. The 802.11 MAC layer in ns2 is used for this purpose. The chosen parameters for simulation are shown in Table I.We describe the simulation for clustering. For cluster formation in the network, we have simulated *on demand clustering.*
On demand clustering is nothing but the AODV protocol. It constructs and maintains the cluster architecture only when there are on-going data. Each node collects neighbor information through DSDV protocol. The cluster-heads are assumed to broadcast their beacons over 2 hops in every 20 seconds time interval. . A gateway is a bridge node that connects two adjacent clusters. The beacon message, sent periodically by a cluster-head

in a cluster, contains information that includes the identifications of the cluster-members, and the gateway node in the cluster. The gateway nodes also send beacons to inform the cluster-members about the adjacent clusters. A node assumes that the nodes it had previously heard from have died or are out of its locality if they have not sent any data within the time-out duration. With a reasonable network communication load, a node can easily keep track of dynamic topology changes by virtue of this time-out.For the purpose of evaluation of the detection efficiency of the system, we have simulated four types of attacks on the network layer. We have assumed that the goal of the attacker is to degrade the performance of the network or individual nodes instead of gaining privileges of a particular node in the network. This assumption means that the proposed IDS focuses on detecting traffic-related attacks. Some of the well-known attacks in this category are: power exhaustion, storage and CPU exhaustion attacks, network bandwidth exhaustion attacks such as flooding and deprivation attacks, routing-disruption attacks such as blackhole and grayhole attacks etc. [19].Table II shows the experimental results obtained from the simulation. It is observed that the proposed system have effectively detected the simulated attacks launched against it at the network layer with a very low false positive rates. In the system me have used two combinational techniques first id AODV based connection establishment due to which no extra time is taken to establish the path between two cluster heads and second is DSDV technique which gives the routing information to the destination node for backtracking.

Table I. Simulation Paramaters

Parameters	Values
Simulation area	500 * 500 m
Number of mobile nodes	30
Transmission range	250 m
Movement model	Random waypoint
Traffic type	CBR (UDP)
Channel capacity	2 Mbps
Total number of flows	15
Avg. packet flow rate	2 packets/s
Packet size	512 bytes/packet
Send buffer at each node	64 packet (fixed)
Training execution time	1000 s
Testing execution time	50 s
Host pause time	5 s

Table II. Performance Results

Attack Type	Detection Rate	False detection Rate
Flooding	100%	2.9%
Blackhole	99.4%	0.2%
Sleep Deprivation	91%	0.6%
Packet Dropping (All)	92%	0.4%

5. CONCLUSION

This intrusion detection system using hybrid approach is a agent based system which forms a cluster head and this head is now used to transfer packets among other nodes. Before transferring the packet , it detect for intruder locally as well globally by broadcasting the key value. In this method it make use of routing table as well Rout Request and Rout Reply Packet .If any intrusion found, it broadcast the massage in the network and uses the secure communication method that is splits the packet and then uses some key to transfer the message. In the system me have used two combinational techniques first is AODV based connection establishment due to which no extra time is taken to establish the path between two cluster heads and second is DSDV technique which gives the routing information to the destination node for backtracking. Hence this system has advantages of little route overhead, short algorithm time; meanwhile, the model has high detection rate, and effectively reduce false detection rate. The simulation test has excellently verified the characteristics above-mentioned.

5. REFERENCES

[1] Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer, Richard A. Kemmerer, "An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks," acsac, pp.16-27, 20th Annual Computer Security Applications Conference (ACSAC'04), 2004.

[2] G. S. Mamatha[1] and Dr. S. C. Sharma[2]"A New Combination Approach To SecureMANETS Against Attacks"International Journal of Wireless & Mobile Networks (IJWMN) Vol.2, No.4, November 2010.

[3] Foong Heng Wai, Yin Nwe Aye, Ng Hian James" Intrusion Detection in Wireless Ad-Hoc Networks" CS4274 introduction to mobile computing.

[4] Sunita Sahu[1] & Shishir K. Shandilya[2"] A Comprehensive Survey On Intrusion Detection In Manet" *International Journal of Information Technology and Knowledge ManagementJuly-December 2010, Volume 2, No. 2, pp. 305-310*

[5] Dorothy E. Denning "An Intrusion-detection Model" *IEEE Transaction on Software Engineering*, **13**, No. 7, Pp 222-232, Feb 1987.

[6] H.–Y. Chang, S.F. Wu and Y.F. Jou, "Real-Time Protocol Analysis for Detecting Link-State Routing Protocol Attacks", *ACM Tran. Inf. Sys.Sec.*, **1**, Pp. 1-36,2001.

[7] O. Kachirski , R. Guha "Effective Intrusion Detection using Multiple Sensors In Wireless Adhoc Networks" HICSS'03, PP 57-64, 2003.

[8] D. Sterne1, P. Balasubramanyam2, D. Carman1, B. Wilson1, R. Talpade3, C. Ko1,R. Balupari1, C-Y. Tseng2, T. Bowen3,

K. Levitt2 and J. Rowe2 "A General Cooperative Intrusion Detection Architecture for MANETs". June 21, 2006 .

[9] Ioanna Stamouli, Patroklos G. Argyroudis, and Hitesh Tewari "Real-time Intrusion Detection for Ad hoc Networks" *Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05),* 0-7695-2342-0/05 $20.00 © 2005 IEEE.

[10] S.Bose,P.Yogesh and A.Kannan "Neural Network Approach for Anomaly Intrusion Detection in Adhoc Networks using Agents" *Internatinal Journal of Soft computing1*, Medwell Online 2006.

[11] Xia Wang " Intrusion Detection Techniques in Wireless Ad Hoc Networks".- 30th COMPSAS 06- 0-7695-2655-1/06.

[12] Yu Liu, Cristina Comaniciu and Hong Man "A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks. – ICC-06, IEEE International Conference, June 2006, PP 2201.

[13] Ningrinla Marching and Raja Datta "Collaborative Technique for Intrusion Detection in Mobile Ad hoc Network" *Ad hoc Networks*, **6**, Issue 4, June 2008 Page 508-523.

[14] Pasquale Donadio, Antonio Cimmino and Giorgio Ventre "Enhanced Intrusion Detection Systems in Ad Hoc Networks using a Grid Based Agnostic Middleware".- AUPC'08, 2nd International Workshop ACM-2008.

[15] S.Madhavi and Dr. Tai Hoon Kim "An Intrusion Detection System in Mobile Ad hoc Networks" *International Journal of Security and its Application*, 2, No 3, July 2008.

[16] S.Sen and John Andrew Clark *"A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad hoc Networks"* March 2009, WiSec '09: Proceedings of the Second ACM Conference on Wireless Network Security.

[17] Yinan Li, Zhihong Qian –"Mobile agents-based intrusion detection system for mobile adhoc network" , PP- 145, 30,31 Jan, 2010 (ICCC-ITOE) .

[18] NS-2 Simulator. URL: http://www.isi.edu/nsnam/ns.

[19] Y.-C. Hu, A. Perrig, "A survey of secure wireless ad hoc routing", IEEE Security and Privacy Magazine, Vol. 2, No. 3, pp. 28-39, May-June 2004.