

An Algorithm for Intrusion Detection and Prevention in MANET

Mrunal Gavhale¹, Pranay D. Saraf²

PG Student, Department of Computer Science, G.H. Rasoni College of Engineering, Nagpur, India¹

Professor, Department of Computer Science, G.H. Rasoni College of Engineering, Nagpur, India²

Abstract: A Mobile Ad-hoc Network (MANET) is self-configured and dynamic network that formed by collecting number of mobile nodes. One cluster consists of group of nodes. It is necessary to have a good and efficient cluster formation and cluster head selection algorithm which will connect other neighbouring node. Their communication should do in very less time. In MANET security is another prime concern. The open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. To prevent from such intrusions need a system which will detects as well as prevent. This system detects and prevents the intrusion in the network on the basis of parameter (such as packet loss ratio, energy consumption, packet delivery delay), once detected restricts that intrusion to enter in the network by blocking the system information of that intrusion and broadcast this information to other cluster head to save energy and protects against Intrusion.

Keywords: Wireless Sensor Network, Cluster, Cluster Head, Intrusion Detection and prevention, Mobile Ad-hoc network (MANET).

I. INTRODUCTION

A Mobile ad-hoc network made up of collection of nodes without help of the centralized management or fixed infrastructure. The networks thus form by mobile nodes and the devices in the network. These devices are able to detect the presence of other devices and perform the necessary set-up to provide proper communications. That's why it is called self-configured network. All Nodes have its own wireless transmitter and receiver called as trans-receiver which allows it to transmit the information which is in its radio communication range. But when it communicates, network topology is changing continuously when the node moves inside the cluster, outside the cluster. Topology used for transmitting the information. While transmitting information with foreign node there may be chance of getting contact with malicious node.

So security becomes prime concern. Intrusion Detection system (IDS) is one of the processes, which monitor the activity of nodes in the network. An IDS gathered activity of information and then analyses it to determine whether there are any activities that violate the security rules. ID determines an unusual activity, it alert Cluster Head to initiate proper response against malicious node. Although there is several intrusion detection techniques developed for wired networks today, they are not suitable for mobile ad-hoc networks due to the differences in their characteristics. Therefore, those techniques must be updated or new techniques must be implemented to make intrusion detection work effectively in wireless ad-hoc networks.

This system designed network by creating a cluster and a cluster head (CH) in each cluster. For selecting Cluster Head (CH) in Cluster, designed new algorithm named as Static-Cluster Head. In which one node selected as Cluster

Head on the basis of energy parameter. That CH becomes Static one in this Cluster and other nodes are dynamic. Each dynamic node registered themselves with CH and getting its own unique ID. Through unique ID CH can identify the nodes in their Cluster. If foreign nodes try to enter in network, The CH collects the information & its activity of intrusion attack in the cluster. It will store the information with the help of parameters, restrict them in the cluster and send the copy of intrusion detection parameters to the other cluster head. So, that other CH, also restrict the intrusion in the next cluster i.e all the cluster head block that particular intrusion node in whole network. In this way the project work successfully detect the malicious node and prevent it from spreading its activity. This reduces energy consumption, delay rate and increases packet delivery ratio.

II. RELATED WORK

The previously existing technique of Intrusion Detection for ad-hoc wireless network is using self-organizing map, in which allocation of weight or training & detection of malicious node is used to detect attack. It is given by V. Dinesh Kumar, Dr. S. Radhakrishnam [1].

This article is given a long process of finding the malicious node "Intrusion detection in MANET using self-organizing Map". The model deals with different types of attacks and their detection approach based on SOM model. The author G. Naga Satish, Ch. V. Ragnavendran, Prof. P. Suresh Varma [2] implemented "Intrusion detection & prevention in wireless ad-hoc network" in which they suggest Intrusion detection can be defined as the automated detection & subsequent of an alarm to alert the security apparatus at a location of intrusion. Responsibility

of Each node in the network is identifying the sign of intrusion, monitoring the system activity, user activity & data transmission activity in the radio range. "EAACK- A Secure Intrusion detection System for MANET" by Elhadi M. Shakshuki, Nan Kang & Tarek R. Sheltamicpropoeed system, when the source send message to the destination through the different nodes the destination sends the acknowledgment to the source through the same node this concept is EAAC (Enhanced Adaptive Acknowledgement). After sending message it waits for acknowledgment for a predefined time period. If acknowledgment not received it switches to secure acknowledgement mode. "Intrusion Detection System in wireless ad-hoc networks based on Mobile agent technology" by AmiraHamdiShaban, HeshamElZouka, MohmadAbouElNasr. In this wireless network they maintain routing table for communication purpose. But it has main problem of time and security. R. Nakkeeran, T. Aruldoss Albert proposed in "Agent based efficient Anomaly Intrusion Detection System in Ad-hoc networks" in which they explained each system has its own home agent which will monitor the activity of its own system. If any node wants to transfer data, first he has broadcast the message to its next and previous node.

Here mobile agent used for collecting the neighboring node information. but home agent is not perfect solution for network security. "Enhanced intrusion detection techniques for mobile ad-hoc network" by by L. PremaRajeshwari, R. Arockia Xavier Annie, A. Kannan. Proposed system is designed to find resource consumption attack, packet dropping attack & fabrication attack[8]. "Network Intrusion system on wireless mobile adhoc networks" by ChilakalapidiMeherBabu, Dr.Ujawal A. Lanjewar design system for intrusion detection for DDoS in packet drop rate, end to end delay, routing load only [10]. But to make network strong we have strong algorithm for Cluster formation and Cluster Head (CH) selection. For this we study the work of Lowest ID(LID), Highest Degree(HD), Low Energy Adaptive Cluster Hierarchy (LEACH). The LID algorithm work by selecting select lowest_id node as CH, by by Hao Wu & ZhangduiZhong, LajosHanzo&Kirtikumar K. Patel, Dhadesugoor R. Vaman [13,14].]. Highest Degree algorithm select the highest degree node as CH, by Hao Wu & ZhangduiZhong, LajosHanzo [13,15], but it face the problem with increase in load. If the network is heavily loaded then throughput of network drops. LEACH select cluster head randomly by performing rounds, in this concept only two node active at a time [14,15,16] by, M.J.Handy, M. Haase, D. Timmermann & LalitaYadav, Ch. Sunitha.

III. PROPOSED METHODOLOGY

A simple wireless network is formed by connecting number of nodes with each other. When nodes are in network they broadcast their presence by sending their ID. But when they broadcast information they faces problem with energy consumption, delivery ratio, and security

occurs in the network. The algorithm Lowest ID (LID) is used for Cluster formation and selection of CH. In this algorithm unique ID is provided to each node and then broadcast throughout the network. So they communicate through their ID. Then to select Cluster Head all ID compared with each other. Among those who have lowest ID will be selected as CH for that particular Cluster. Same process continues in all Cluster of the network, while its single hop neighbour's become the cluster member. This algorithm is simple to understand but complicated to implement. The CH is undesirably high. The problem of LID algorithm packet delivery delay is excessive. For C selection only ID's are considered, no other qualification require[13]. The second algorithm is Highest Degree Clustering Algorithm, in which node which is having highest connectivity or more number of other nodes communicate with that node then this node will be CH for that particular Cluster. It means those nodes having highest degree it will be selected as a Cluster Head. If the network increases, load is also increases and the problem of bottleneck also increases likewise throughput decreases [13]. Another algorithm is LEACH (Low Energy Adaptive Clustering Hierarchy), in this selection of CH is done on the basis rounds. At a time only two nodes are active which will transmit to data to each other. But it required too much time to send data because at a time only two nodes are active so others have to be ideal. This algorithm is good for small network [14,15].

In this research work design a system for mobile ad-hoc wireless network by defining Cluster and Cluster Head. The number of nodes collect together formed a group known as cluster and by collecting number of cluster formed a network. The all nodes in the cluster are dynamic but only one node which is CH for that network is Static in nature. Each node has its own ID so they are identified through their ID. As the CH of that network is Static so the new algorithm named as STATIC-CH (S-CH) algorithm. In this algorithm CH is selected at the time of network creation and this CH will be Static throughout the network. Others nodes are dynamic and working as a Cluster member. Firstly all the nodes registered themselves to CH and he provided them a unique ID. Cluster member broadcast their ID to the network so that all members have the idea of its previous and next cluster member. If the receiving node receives the same packets again & again then receiving node drop this same packet, even if the CH also receives the same packet from registered sender node then CH will also drop the same packets. The CH broadcast the information of register nodes & the data to the other CH in the mobile ad-hoc wireless network so that if the same nodes register with previous CH goes in to the radio range of other CH. And node wants to access the information of other CH, CH allow him to do so. Because of Static CH energy degradation problem solved. This reduces the energy consumption, error rate, packet delay rate & increase delivery rate as time requirement for accessing the information is less, it can access the nearest CH information easily. If the intrusion node broadcast same

messages again & again to the other node in the same cluster it is detected by CH & the receiving node drops the packet sent by intrusion node. After that CH will block its physical address or MAC address to that cluster and also send this information to other nearest CH. As soon as they get any request from this node they can block that malicious node easily.

IV. EXPERIMENTAL DETAILS

A. Creation of Cluster and CH

Each wireless ad-hoc network have some radio rang and Cluster also have radio range. If one node is registered in Cluster - 1 now it moves from Cluster -1 to Cluster -2, wants to access the information from Cluster -2. For this we proposed a new algorithm i.e. S-CH (Static-CH) for creation of Cluster and selection of CH which will then compared with LID, HD, LEACH algorithm. In this module cluster & one CH in each cluster will be created using Network Simulator-2.34 (NS-2.34). Radio ranges in the wireless network indicated by the circles & the nodes that in the range of radio range are considered as the node in that particular cluster. The following are the simulation parameter.

TABLE I: PARAMETER TABLE

Parameter	Values
Channel Type	Wireless Channel
Radio Propagation Model	Two Ray Ground
Antenna Type	Omni Antenna
Number of nodes	50
Network Interface Type	Wireless_phy
Mac Type	Mac/802_11
Routing Protocol	SADV
Link Layer Type	LL

B. Detecting Intrusion in the network.

In the system Intrusion Detection Parameter are used to find out intrusion in the network.

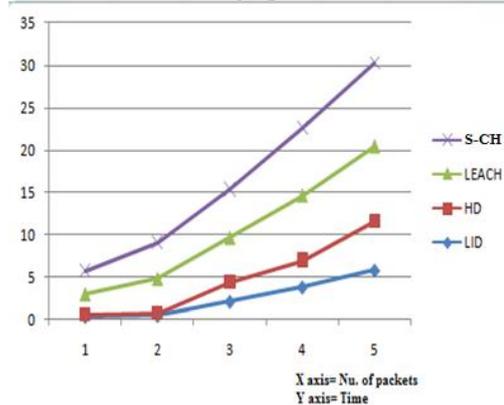
It helps to maintain information about intrusion node if any node seems to violate the activity of system; CH stores the information and broadcast same information to the other CH to prevent from malicious node.

As soon as other Cluster Head comes to know that this node is malicious one, then other CH checks its parameter if it exactly matches to intrusion parameters, stores the address and restrict malicious node to enter in the network. The parameters required for detecting intrusion is related with the system configuration of the computer.

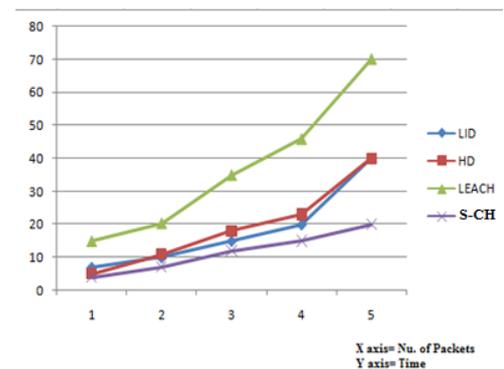
This process helps to find out intrusion in the network. But to declare node as an intrusion we have to calculate some value i.e. behaviour of system and calculate average value. If this average value is greater than the range we defined then the node is declare as malicious node first time.

V. RESULT & DISCUSSION

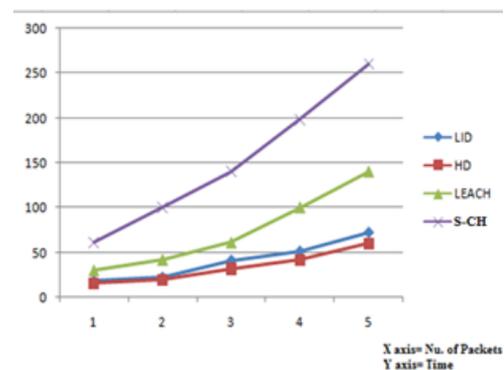
The simulation did on Simulator-2.34 (NS-2.34). The final result compared with algorithms LID, HD, LEACH. The result shows in the form of graph.



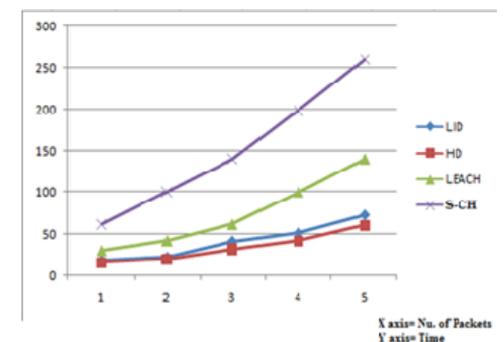
Graph 1: Packet Delivery speed



Graph 2: Error Graph



Graph 3: Packet Delivery Rate Graph



Graph 4: Delay Graph

Above graph shows the comparison result of algorithms. This comparison shows the performance of new S-CH algorithm.

VI. CONCLUSION

This paper proposed new scheme for creating Cluster and selecting CH by comparing LID, HD, LEACH. The Algorithm defined some parameter to declare node as malicious or intrusion node. Most of existing intrusion detection system detects the intrusion in variety of way but there are many problems arise with security & transmission of messages between the nodes. In this system we tried to resolve the problem of energy consumption. We also worked on to minimize the delay rate, error control rate and increase packet delivery ratio. As we proposed S-CH (Static-CH) algorithm, it will be a great future work in considering designing cluster, CH & also this system is very much useful for detecting intrusion in ad-hoc wireless network in future.

REFERENCES

- [1]. V. Dinesh Kumar, Dr. S. Radhakrishnan "Intrusion Detection in MANET using Self Organizing Map (SOM)" International Conference on Recent Trends in Information Technology
- [2]. G. Naga Satish, Ch. V. Raghavendran, Prof. P. Suresh Varma, "Intrusion Detection & Prevention in Wireless Ad-hoc Network", International Journal of Advanced Research in Computer Science & Software Engineering volume 3, Issue 4, April 2013.
- [3]. Elhadi M. Shakshuki, Nan AKng&Tarek R. Sheltami, "EAACK-A Secure Intrusion Detection System For MANETs", IEEE transaction on industrial electronics, vol 60, no.3, MARCH 2013.
- [4]. AmiraHamdiShabaan, HeshamElZouka, Mohamed AbouELNasr, "Intrusion Detection System in Wireless Ad-Hoc Networks Based on Mobile Agent Technology", IEEE 2010
- [5]. R. Nakkeeran, T. AruldasAlbert& R. Ezumalai, "Agent Based Efficient Anomaly Intrusion Detection System in Ad-hoc Networks", IACSIT, International Journal of Engineering& Technology Vol. 2, 1 Feb, 2010
- [6]. ArockiaTubi. S, Vairachilai, "A Survey on Intrusion Detection System in Mobile Ad-hoc Networks", IJCSMC Vol. 2, Issue 12, December-2013
- [7]. L. PremaRajeswari, R. Arockia Xavier Annie, A. Kannan, "Enhanced Intrusion Detection Techniques For Mobile Ad-Hoc Networks", International Conference on Information & Communication Technology in Electrical Science
- [8]. Chilakalapudi MeherBabu, Dr. Ujwal A. LAnjewar, Chinta Naga Manisha, "Network Intrusion Detection System on Wireless Mobile Ad-hoc Networks", International Journal of Advanced Research in Computer & Communication Engineering vol.2, Issue 3, March 2013.
- [9]. Hao Wu &Zhangdui Zhong, LajosHanzo, "A Cluster-Head Selection & Update Algorithm for Ad Hoc Networks".
- [10]. M. J. Handy, M. Haase, D. Timmermann, "Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection", IEEE 2002
- [11]. LalitaYadav, Ch. Sunitha, "Low Energy Adaptive Clustering Hierarchy in Wireless Sensor Networks (LEACH)", IJCSIT 2014.
- [12]. Sayani Chandra, IspitaSaha, Poojarini Mitra, BidyutmataSaha, Sinthai Roy "A Brief Overview of Clustering Schemes Applied on Mobile Ad-hoc Networks" International Journal of Advanced Research in Computer Science and Software Engineering, Vol.5, Issues 2, Feb 2015
- [13]. Hao Wu and ZhangduiZhong, LajosHanzo" A Cluster-head Selection and Update Algorithm for Ad Hoc Networks" 978-1-4244-5637-6/10/\$26.00 ©2010 IEEE
- [14]. Damianos Gavalas, Grammati Pantziou, Charalampos Konstantopoulos, Basilis Mamalis "Lowest-ID with Adaptive ID Reassignment: A Novel Mobile Ad-hoc Network Clustering Algorithm"
- [15]. "A Modified Lowest ID Algorithm For practical wireless clustered Network" <http://www.researchgate.net/publication/280065537>
- [16]. Mohini Kumrawat, Manoj Dhawan" Survey on Clustering Algorithms of Wireless Sensor Network" International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2046
- [17]. Chunyao FU, Zhifang JIANG, Wei WEI and Ang WEI "An Energy Balanced Algorithm of LEACH Protocol in WSN" IJCSI International Journal of Computer Science Issues, Vol. 10, Issues 1, No 1, Jan 2013
- [18]. V. Dinesh Kumar, Dr. S. Radhakrishnan "Intrusion Detection in MANET using Self Organizing Map (SOM)" International Conference on Recent Trends in Information Technology 2014.

BIOGRAPHY



Mrunal Gavhale received the bachelor's degree in Computer science and engineering from the Nagpur University, Maharashtra, India in 2013. Presently she is pursuing her master's in mobile technology in the department of Computer Science from G. H. Raisoni College of Engineering, Nagpur Maharashtra, India. Her research interests include wireless sensor networks, intrusion detection, network security, wireless security etc.