ISSN:0975-9646

An Algorithmic Approach for the Detection of Malicious Nodes in a Cluster Based Adhoc Wireless Networks

Bhakti Thakre[1], S.V.Sonekar[2]

[1.] Research Scholar, [2.] Professor, Head of Department,
Department of CSE,
J D College of Engineering and Management,
Nagpur M.S., India

***Abstract*— Mobile ad hoc networks (MANETs) are an infrastructure-less, dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. The network nodes in MANET are free to move randomly therefore, the network topology of a MANET may change rapidly and unpredictably. Due to the dynamic change in topology finding a better route is very difficult. Some nodes misbehave as they participate in route establishment phase but refuse to forward the data packets to reverse their own energy.**

These networks can be setup easily anywhere and anytime without any base infrastructure, thus they have proved to be very efficient is rescue related areas like flood and fire. MANETs are now extended to be used in military and law enforcement. MANETs still face the major problem of security and privacy, especially when used in sensitive areas of computing. To provide better security a secure routing protocols have been developed to provide various levels of security and privacy in this area [2].

***Keywords*— MANET, 2 ACK, Ad Hoc Networks, Cluster head (CH), DSDV, DSR, RREQ, RREP, Routing Protocols Security.**

I. INTRODUCTION

MANET's are self-organisable and configurable hence also known as multi hop wireless ad hoc networks, where the topology of the network keeps on changing continuously. A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which interact with each other through wireless links either directly or depending on other nodes such as routers. The procedure of MANET is not depending on existing base stations or infrastructure Network clients in MANET may move freely and randomly. Therefore, the network topology of a MANET can be change unpredictably and speedily. All network activities, for instance forwarding data packets, and topologies for detecting which concern with nodes themselves for execution either collectively or independently.

In Route Discovery process, the source node generate RREQ packet, if the path to destination is not stored in the routing table, and pass it to the neighboring nodes. The neighboring nodes will pass it to their neighbor and so on. When the packet reached to the destination node, then destination node generates RREP (Route Reply) packet and send it back to the source node. Thus the path is established between source and destination node [1].

In Route Maintenance process, the source node is up to date by RERR (Route Error) message in case of link failure.

The Maximum-Lifetime routing approach emerges for the nodes that have minimum energy so that they can be eliminated from the path [8].

Routing protocols in Mobile Ad hoc Network (MANET) send periodic messages to realize the changes in topology. Sending periodic messages cause overhead. Compared to proactive routing protocols, reactive routing protocols can cause less overhead. Broadcasting can cause broadcast storm problem .To discover the route better than broadcasting methodology rebroadcast can done with the help of neighbor knowledge methods. We also define a connectivity factor to provide the node density adaptation. This approach can significantly decrease the number of retransmissions so as to reduce the routing overhead and also improve the routing performance. Thus finding the neighborhood node, we use channel awareness mechanism for data transmission and to improve the quality [7].

In mobile ad hoc networks (MANETs), nodes usually cooperate and forward each other’s packets in order to enable out of range communication. However, in hostile environments, some nodes may deny to do so, either for saving their own resources or for intentionally disrupting regular communications. This type of misbehaviour is generally referred to as packet dropping attack or black hole attack, which is considered as one of the most destructive attacks that leads to the network collapse [9].

Mobile Ad Hoc Network (MANET) can be described as an autonomous collection of mobile nodes (users) that communicate over relatively low capacity wireless links, without a centralized infrastructure. In these networks, nodal mobility and the wireless communication links may lead to dynamically changing and highly unpredictable topologies. All network functions such as routing, multi-hop packet delivery and mobility management have to be performed by the member nodes themselves, either individually or collectively.

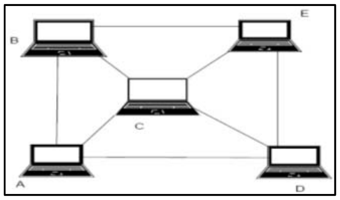

Fig.1 Mobile Adhoc Networks

Consider the above Fig. 1, if node A wants to communicate with B, D or C it can act together directly because all the three nodes are within the range of A and therefore it can establish a direct link between them whereas if A is willing to communicate with E it cannot directly do so because E is not within the range of A and therefore A has to take help of either C, D or B. Therefore this communication between A and E is known as multi hop communication.

This paper is organized as follows: review of previous work in Section 2, In Section 3, we describe Clustering algorithm in detail , In Section 4, we provide expected results; Section 5 concludes the paper.

II. Literature Survey

A Mobile Adhoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other.

In mobile ad hoc networks, the movement of the network nodes may quickly changes the topology which results in the increase of the overhead message in topology maintenance. Protocols try to keep the number of nodes in a cluster around a pre-defined threshold to facilitate the optimal operation of the medium access control protocol. The cluster head election is invoked on-demand, and is aimed to reduce the computation and communication costs. A large variety of approaches for ad hoc clustering have been developed by researchers which focus on different performance metrics.

By classifying nodes into clusters, the proposed scheme allows each Cluster Head (CH) to detect false accusation by a Cluster Member (CM) within the cluster. Node clustering provides a means to mitigate false accusations.

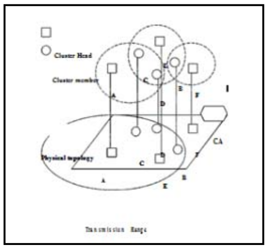

Fig. 2 Node clustering

Fig2 shows how clusters are constructed in the proposed scheme. While each cluster consists of one CH and CM lying within the CH's transmission range, some nodes within the transmission area of the CH might not be the member of the cluster and can be the CM of another cluster [4].

In this proposed scheme, every node in the network monitors the behavior of its neighbors, and if any abnormal action is detected, it invokes an algorithm to determine direct trust value [6].

Ad-Hoc network routing protocols are commonly divided into three main classes; Proactive, reactive and hybrid protocols. In proactive routing, each node has to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. In Reactive Protocols, Reactive routing is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. In Hybrid Protocols, a hybrid model that combines reactive and proactive routing protocols [3].

III. Algorithms

There are numbers of Clustering Algorithms like Identifier based clustering, Connectivity based clustering, Mobility aware clustering.

In this paper we will discuss the clustering algorithm based on highest connectivity clustering. The degree of a node is computed based on its distance from others. Each node broadcasts its id to the nodes that are within its transmission range. The node with maximum number of neighbors (i.e., maximum degree) is chosen as a cluster head (CH).

The neighbors of a cluster head become members of that cluster and can no longer participate in the election process. Since no cluster heads are directly linked, only one cluster head is allowed per cluster. Any two nodes in a cluster are at most two hops away since the cluster head is directly linked to each of its neighbors in the cluster. Basically, each node either becomes a cluster head or remains an ordinary node.

As MANET typically lack a central authority for authentication and key distribution, security mechanisms must be scalable and capable of frequent topology changes. In this section we proposed cryptography based secure technique to handle malicious node in MANETs.

In this paper we will discuss highest connectivity Clustering Algorithm for cluster Head selection. In this Algo we will create a table having the fields Name, Index, ID, X Coordinate, Y Coordinate. The ID of the node will be taken from the system which is system generated and inform the server as a node in the range of that server.

The Highest Connectivity Clustering Algorithm

1. Each node in the network is assigned a pair of parameters, the connectivity of the node and its identifier.
2. A node is selected as a cluster head if it has the highest connectivity. If two or nodes have the same

connectivity, the second criteria - the lowest ID priority is checked to find the cluster head.

3. The idea is that every node broadcasts its clustering decision once all its k- hop neighbors with larger cluster head priority have been done.

Now, we will analyze a performance of clusters based on the number of nodes i.e., density of a cluster.

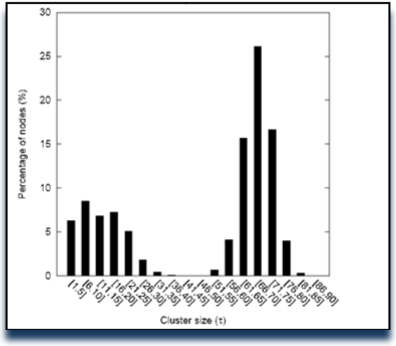

Fig. 3 Distribution of Cluster Size for 90 nodes over 25000 scenarios.

Fig 3 shows the distribution of the cluster size for a network of n= 90 nodes with node density of cluster v = 25. This distribution is obtained by averaging the simulation results of 25000 random network scenarios. The CH are selected according to the distance-2 constraint, *i.e.* each node is either a CH or is within 2 hops from a CH. The x- axis shows the size of clusters and the y -axis the percentage of nodes being in a cluster of that size. This percentage is calculated over 90 nodes and over 25000 random scenarios that we simulated. As the size of cluster increases the performance goes decreases.

The result shows that if some clusters are too large and the CH have to relay a high amount of control traffic for their dependants then congestions may occur in the network. It can directly impact the network's quality of service

We can observe in the above graph that the cluster size's distribution is highly uneven: 62% of nodes in the network are in clusters that have more than 60 dependants, whereas 29% of nodes are in clusters that only have 20 dependants or less. With the majority of nodes being dependants of large clusters, the network traffic can be congested due to the bottlenecks at the CH.

The node which is having the highest connectivity means the node that is having the ability to communicate with maximum number of nodes will be selected as a Cluster head.

Here we are using ALOHA protocol for sending data from source to destination. We have made comparison with different routing protocols like DSDR, DSR etc.

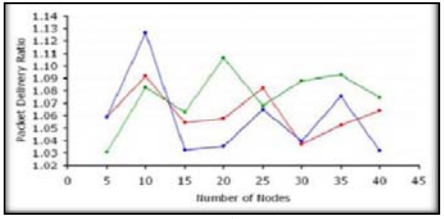

Fig. 4 Packet delivery ratio for ALOHA, DSR, DSDV

In terms of packet delivery ratio in Fig. 4, Dynamic Source Routing (DSR) Protocol i.e. (Blue Line in Fig.4) performs well when the number of nodes is less means when the load is less. However its performance declines with increased number of nodes due to more traffic in the network. The performance of Destination Sequenced Distance Vector DSDV Protocol i.e. (Green Line in Fig. 4) is better with more number of nodes than in comparison with the other two protocols. The performance of ALOHA Protocol i.e. (Red Line in Fig.4) is consistently uniform.

IV. Expected Results

In this paper we proposed, a better solution for energy saving process by improving quality in selection of cluster Head from the nodes in the cluster which are best fitted for routing in between wireless nodes.

In the omnetpp simulation, we will create four clusters having name A,B,.C and D. In each cluster there will be one static not which must be in the range of the server in a cluster. Once the self message is called for server and static node then only the communication begins. Cluster is formed and the cluster head will be elected using the higest connectivity clustering algorithm. In each cluster there will be only one clusterhead. The elected clusterhead from the algorithm will communicate with other clusterheads in the network.In fig 5 it is shown that there is one server in the cluster and one static node is present in the range of server of cluster A. At leaset one node is necessary to be present in the cluster. Other nodes are movable ie. they are moving from one cluster to another.

Fig. 5 Snapshot of Static Node in Cluster A

The nodes which move in the cluster our Highest Connectivity Clustering Algo will check the Connectivity of the nodes. The node with the highest connectivity is declared as a Cluster head who will communicate with other clusters in the network.

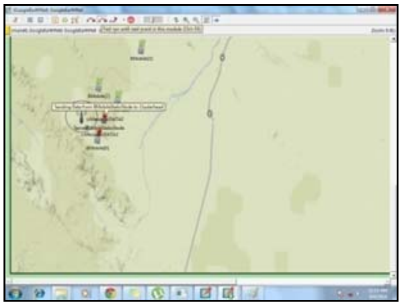

Fig. 6 Snapshot of Sending Data to Cluster head

In fig.6 the Static node in cluster B will send the data to cluster Head. Basic parameters like energy carrying capacity, buffer size, speed of nodes, mobility rate and average error rate for a protocol like AODV have been monitored to have changes for desired results [1].

Fig. 7 Snapshot of Cluster

In fig. 7, the server in the cluster will send the message to the static node which must be present in the range of the server.

If any clusterhead will detect the malicious node in his cluster he will inform another clusterhead to stop that particular node entry in their cluster to aviod packet dropping.

V. Conclusion

The attack schemes, as well as prevention, detection and reaction mechanisms have been explored. We categorized them into three categories according to their goals and their specific strategies. A comparative study between them was then conducted to highlight their respective effectiveness. We concluded that most of the algorithms are proposed but we are using the Connectivity based algorithm for selecting the cluster head which will effectively communicate with other cluster members.

In this paper, investigation is done on the election of cluster head for better communication between the nodes in the cluster and find out the misbehavior of nodes and a new approach is proposed for detection of cluster head (CH). Suggested approach can be united on top of any source routing protocol such as ALOHA and is based on sending acknowledgement packets for reception of data packets and using promiscuous mode for counting the number of data packet such that it overcomes the problem of misbehaving nodes. In any complex distributed system of nodes, clustering of nodes into groups results in simplification of addressing and management of the nodes and also yields better performance since details about the remote parts of the distributed system can be handled in a proper way. In future we can detect the selfish nodes who are not forwarding the message to save their own energy.

References

[1] Abhilash Sharma and Birinder Singh, “Fault Tolerance with Clustering Approach in Ad-Hoc on Demand Protocol”, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 9, September – 2013.

[2] Namrata Marium Chacko, Getzi P. Leelaipushpam, “A Reactive Protocol For Privacy Preserving Using Location Based Routing In Manets”, IJCSN International Journal of Computer Science and Network, Vol 2, Issue 2, April 2013

[3] Aarti , Dr. S. S. Tyagi “ Study of MANET: Characteristics, Challenges, Application and Security Attacks " , International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013

[4] Ms.T.R.Panke, “Clustering Based Certificate Revocation Scheme for Malicious node in MANET “, International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013

[5] Manoj V. Mori1, G.B. Jethava,“Node registration in MANET”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 1 January - February 2013.

[6] Aravindh S, Vinoth R S and Vijayan R, “A Trust Based Approach For Detection And Isolation Of Malicious Nodes In Manet”, International Journal of Engineering and Technology (IJET) Vol 5 No 1 Feb-Mar 2013.

[7] V.Deeban Chakravarthy, V.Divya Renga , “A Neighbor Coverage Based Probabilistic Rebroadcast For Reducing Routing Overhead In Mobile Ad Hoc Networks”, International Journal of Emerging Technology and Advanced Engineering Volume 3, Special Issue 1, January 2013.

[8] Tripti Nema , Akhilesh Waoo , P.S.Patheja , Dr.Sanjay Sharma ,” Energy Efficient Adaptive Routing Algorithm in MANET with Sleep Mode”, International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-2 Number-4 Issue-6 December-2012.

[9] Soufiene djahel, farid abdesselam and zonghua zhang, “Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges”, IEEE communications surveys & tutorials, vol. 13, no. 4, fourth quarter 2011.

[10] Daniel Camara Antonio , A.F. Loureiro, “A Novel Routing Algorithm for Ad Hoc Networks”, Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000.