DESIGN AND DEVELOPMENT OF AN ALGORITHMIC APPROACH FOR SELFISH AND MALICIOUS NODE IN CLUSTER BASED ADHOC WIRELESS NETWORKS

Bhakti Thakre¹, S.V.Sonekar²

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

ABSTRACT

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes such as routers. 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 route is very difficult. Some nodes misbehave as they participate in route establishment phase but refuse to forward the data packets to conserve their own energy. For detecting routing misbehavior in MANET lots of techniques are there such as watch-dog, path rater, TWOACK, End to End ACK scheme. But due to few disadvantages in the above scheme we propose a new scheme called 2ACK.

Mobile Ad hoc networks (MANETs) are an infrastructure less, self configuring network. 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. Secure routing protocols have been developed to provide various levels of security and privacy in the past.

Keywords: 2 ACK, AODV, MANET, Packet Dropping Attack, RREQ, RREP.

1. INTRODUCTION

The MANETs, as a technology for dynamic wireless networks, had been deployed in military since 1970s, and thereafter it had been applied in various applications such as; patient monitoring, airplane exhaustion breakage supervision, business associates sharing information during a meeting;
attendees using laptop computers to participate in an interactive conference, remote landscapes monitoring, and emergency disaster relief personnel coordinating efforts after an earthquake [1].

Aloha Protocol transport capacity is proportional to the square root of the density of mobiles which is very impressive. Finally, this protocol is self-adapting to the node density and it does not require prior knowledge of the density [2].

Other protocols like AODV can also be used for finding the route in the network. AODV protocol is a reactive routing protocol which finds route to destination when required. It consists of routing table which helps to differentiate between expiry and fresh routes. The routing table at node contains the sequence number and next hop information.

The working of protocol is consists of two phases:
1. Route discovery
2. Route maintenance.

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 [4].

In Route Maintenance process, the source node is up to date by RERR (Route Error) message in case of link failure. There are two main factors that cause link failures are:
1. Battery life time.
2. Mobility.

There are three methods that are used to achieve the energy-efficiency in MANETs Energy-Control, Energy-Save and Maximum-Lifetime routing. The Energy-Control approach is permitting nodes to decide the least amount of transmission power level which is adequate to maintain network connectivity and to pass the traffic with less energy, the objectives is to increase network capacity and declining energy consumption. The Energy-Save approach deals with the power loss during the idle mode and this can be minimized by increasing the amount of time a node spends in the sleep mode. Finally, the Maximum-Lifetime routing approach emerges for the nodes that have minimum energy so that they can be eliminated from the path.

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. The 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 [10].

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 [11].

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.

![Image](image_url)

**Figure 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 Routing algorithm in detail and then explain a Selfish and Malicious node used in MANET. In Section 4, we provide expected results; Section 5 concludes the paper.

## 2. LITERATURE SURVEY

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.

Mobile Ad hoc Network (MANET) do not have any fixed infrastructure and consists of wireless nodes that move dynamically without any boundary limitation. MANETs are advantageous because they are quick to install, provide fault tolerance, connectivity and mobility.

There are three types of selfish nodes as follows:

1. **Selfish Nodes Type 1 (SN1)** - These nodes participate in route establishment but refuse to forward data packets (which are usually much larger than the routing control packets).
2. **Selfish Nodes Type 2 (SN2)** - These nodes participate in neither the route establishment phase nor forward data packets. They only use their energy for transmissions of their own packets.
3. **Selfish Nodes Type 3 (SN3)** - These nodes behave (or misbehave) differently based on their energy levels.

When the energy lies between full energy $E$ and a threshold $T_1$, the node behaves properly. For an energy level between $T_1$ and another lower threshold $T_2$, it behaves like a node of type SN1. Finally, for an energy level lower than $T_2$, it behaves like a node of type SN2. The relationship between $T_1$, $T_2$, and $E$ is $T_2 < T_1 < E$. The existence of the SN2 type nodes is simply ignored by the routing protocol [3].

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.
Figure 2: Node Clustering

In fig 2 shows how clusters are constructed in the proposed scheme. While each cluster consists of one CH and CMs 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].

Cluster-based routing is a solution to address nodes heterogeneity, and to limit the amount of routing information that propagates inside the network. The idea behind clustering is to group the network nodes into a number of overlapping clusters. Clustering makes possible a hierarchical routing in which paths are recorded between clusters instead of between nodes. This increases the routes lifetime, thus decreasing the amount of routing control overhead. Inside the cluster one node that coordinates the cluster activities is cluster head (CH) [12].

Figure 3: Detection and Reaction Using TRUST (DRUT)
In fig 3 Cluster head is finding the TRUST value which will satisfy some rules. If any node does not satisfy the condition then it will be declared as a malicious node.

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 [9].

There are three types of attacks that are:
1. Black hole attack: Once it receives the packets it simple discards them without forwarding to the destination. This attack results in huge loss of data.
2. Man-in-The-Middle Attack: The malicious node will remove the keys of a RREQ and add its own keys. It will reply to the sender node as if it is the destination, and then it will generate a new RREQ and forward to the intended destination with its own session key. This attack can go undetected and the malicious node can easily get hold of information being passed.
3. Location Based attacks: Since we are using Location based routing the possibilities of location based attacks increases [5].

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. [6]

3. ALGORITHMS

In Novel Routing Algorithm, message is shared at multiple nodes and then passes through common channel at the destination. We are using this algorithm to make the routing efficient in MANET. The algorithm proposed the scheme to reduce the overhead and network stability. This method also maintains the Data confidentiality at various nodes.

![Figure 4: Host A wants to send a packet to host G and the initial route is shown on the left scenario. In the meantime host C changes its location as shown on the right scenario and a new route is chosen.](image)

The fig 4 depicted two possible scenarios in a MANET when host A wants to send a packet to host G. An important aspect of any routing algorithm for MANETs is how the routing table is updated. It is clear that better routes can be determined whenever a host has more recent information about the network configuration. Routing information can be obtained both locally and globally. Local information is obtained from a neighbor node that periodically broadcasts only the changes occurred since the last time [12].
We describe the Rebroadcast delay description for the node $n_i$. This algorithm is used for reducing routing overhead in route discovery [10].

As MANETs 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 propose a cryptography-based secure technique to handle malicious nodes in MANETs. The technique consists of the following steps.

1. There will be a dedicated node called a registration node (RN) and its function will be to generate and assign registration tokens to each and every node.
2. Whenever the two nodes want to communicate with each other, they have to request to RN for a registration token.
3. The request packet will contain source node identity, timestamp, home address, and token request. $RP = (Nid, timestamp, h_addSN, reqR)$
4. When RN receives a request from a source node, first, it will check the node identity and its home address to determine which network it belongs to.
5. After successful confirmation, it generates a registration token and assigns it to the node. The registration token will contain node ID, timestamp, duration, public key, nonce, and that token will be encrypted using the private key of RN.
6. After receiving the registration token by a source node, it sends an ACK signal to RN. The ACK signal will contain the node ID and timestamp. The ACK signal will be encrypted using the public key of RN.
7. Steps 3-6 will be carried out between the destination node and RN too.
8. After getting the registration token from RN by both source and destination nodes, they can proceed with their communication.

In the above eight steps, it is clearly mentioned that without getting the registration token, no communication can be initiated between nodes [8].

2 Ack Scheme works with three nodes in which source sends a packet to the first node, and then that node sends the information to the next node. Similarly, node N1 in the figure sends a packet to node N2, and similarly to node N3. After receiving the packet, these nodes will send the acknowledgement packet to the previous node.

The triplet $N1 \rightarrow N2 \rightarrow N3$ is used as an example to illustrate the 2ACK Scheme. One thing that codes execute on each of the sender/receiver of the 2ack packets: Data Packet Sender Side Algorithm (Node N1) Find all the active nodes. Find all routes between the active nodes. Choose the destination node. Get the path to the destination from the routing table. If Yes then send the data packet to the destination. If No - Destination is unreachable. After sending the Data packet, start the timer and wait for the ACK (acknowledgment) of the third node in the opposite path as sent. After the timer expired.

![Figure 5: Working of 2 Ack Scheme](image-url)
check for the ACK (acknowledgment). If the ACK has not come then corresponding node attached to that link declared as misbehaving node.

2 Ack Packet Sender Side (Node N3) Algorithm works like as given below:

1. Cpkts—>0, Cack—>0, i, n //Initialization at node N3
2: while true do
3: if (data packet received) then
4: Cpkts ++ // Increase the counter of received packets
5: if (Cack/Cpkts <Rack) // The data packet needs to be acknowledged
6: Prepare 2ACK
7: Send 2ACK
8: Cack ++, i - - //Increase the counter of acknowledged packets
9: end
10: end
11: end

Here, Cpkt is the variable used to count the no of packets received by the node. Cack will count the no of acknowledgement received from the node. Whereas Rack is defined as a ratio of the total number of data packets acknowledge to the total number of Data packets received.

In this paper Novel routing algorithm is used in which we will send the packet to each and every node present in the cluster. If any of the nodes failed to send the acknowledgement of the packet then the algorithm will choose the alternative path on which source has already send the packet. Whenever a mobile node wants to join the MANET, it listens to the medium to find out a neighbor node n. Once a neighbor node n is identified the mobile host sends a request packet to n asking for its routing table which is sent back to the host. From this moment on the new mobile host can start routing and sending packets in the MANET.

The routing protocol is based on the physical location of a destination host d stored in the routing table. If there is an entry in the routing table for host d, the best possible route is chosen using a shortest path algorithm. The route comprised of a list of nodes and the corresponding TTL’s, is attached to the packet which is sent to first-host in the list. If host d is not found in the routing table, the mobile node sends a message to the nearest fixed node that tries to find the destination node. In Fig 6, Host A wants to send a packet to host G and the initial route, while in the meantime host C changes its location and a new route is chosen.

In any Cluster the most important member is Cluster Head. Only Cluster Head will communicate with another cluster Head for communication.ACO is an evolutionary algorithm. It is inspired by the foraging behavior of ants. The ants release chemical called pheromones on the path while moving along the path. As more number of ants moves along the path, the pheromone concentration increases. The more the pheromone concentration, more is the chance for a new ant to choose that path to reach the food from the colony. The path chosen by the ants will be the shortest path from nest to food. The process is a kind of distributed optimization mechanism, in which they find the shortest distance from the food to colony.

An ACO (Ant Colony Optimization) Algorithm is used for selecting cluster head from the cluster of n nodes.

1. Initialize each node
2. weight=0
3. isHead=false
4. pheromone=0
5. Convecto=empty //To store al neighbor nodes According to instantaneous topology.
6. Find neighbor //nodes in Range
7. If Euclidian distance < Range
8. Edge exists
9. Else
10. No edge exists
11. Increment weight // connectivity measure
12. Set α, β values // control parameters
13. Iterate i to n times
14. Select i\textsuperscript{th} node as Cluster head
15. Select neighbor with maximum probability as next cluster head until all nodes are covered.
16. Update pheromone of the selected cluster heads
17. Find final set of cluster heads with maximum probability (with Weight and Updated pheromone).

A node is said to be in the range of another node, if the Euclidian distance between the two nodes is within the range of each other. A hierarchical routing is done using clustering in which paths are recorded between clusters instead of between nodes. This reduces the amount of routing control overhead. ACO finds the minimal set of cluster heads. This is an iterative process and the output obtained is a local solution. Pheromone value associated with each node and its visibility. Visibility refers to the number of nodes that will be covered if the node is added into the cluster head set. Visibility keeps changing as topology changes. The pheromone value associated with a node is updated for each iteration of the algorithm. For each iteration, a node is selected as the cluster head and the next cluster head is selected based on the pheromone and visibility of its neighbor nodes. This process continues until all the nodes in the network are covered. A node is said to be covered if it is a cluster head or falls in the range of an already selected cluster head.

4. RESULT

In this paper we proposed, a better solution for energy saving process by improving quality in selection of nodes which are best fitted for routing in between wireless nodes. The most important parameter used for finding the route is the transmission range of the node. Node who is in the middle of the cluster can transmit the packet for long time. So, that node will be declared as a cluster head of the network. Aloha Protocol is used for transmitting packets because its transmission range is better than any other protocol. Moreover research worked can be done with Time on demand distance vector protocol for further experimentation. After working on Omnetpp we can see the result of 2 Ack Scheme on Omnetpp as shown below.

![Figure 6: 2 Ack simulation on Omnetpp with Aloha protocol](image-url)
In fig 6 A and B shows the Acknowledgement from Host 2 to Host 1 and from Host 1 to Server. Acknowledgement is received from Basic parameters like energy carrying capacity, buffer size, speed of nodes, and mobility rate and transmission range for Aloha have been monitored to have changes for desired results.

In this work first module is 2 Ack Scheme then second module is random selection of malicious node and then Clustering and moving the nodes in the network.

5. 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 and limitations. We concluded that most of the proposed schemes in the first, second or third defense line are based upon certain assumptions that are not always valid due to the dynamic nature of MANETs and their specific characteristics.

In this paper, investigation is done on the misbehavior of nodes and a new approach is proposed for detection and isolation of misbehaving nodes. 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. ACO Algorithm is used to find the effective cluster Head in the cluster.

6. REFERENCES


