Reduction in routing overhead in MANET using 2-ACK scheme and Novel routing Algorithm

Sonali Gaikwad[#1] and Dr. D. S. Adane[*2]

[#]*M.Tech Studednt, Department of Computer Science & Engineering, RCOEM, Nagpur, India.*
[*]*Head, Department of Information Technology, RCOEM, Nagpur, India.*

Abstract **- Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bi-directional wireless links either directly or indirectly. In mobile ad hoc networks (MANETs), nodes usually cooperate and forward each other's data packets in order to enable out-of-range communication. However, in friendly environments, some nodes may refuse to do so, either for saving their own energy or for intentionally disrupting regular communications (i.e. selfish or malicious nodes).This selfish nodes start refusing to forward or drop data packets thereby degrades the performance of the network. This type of misbehaviour is generally referred to as packet dropping attack or black hole attack, which is considered as one of the most critical attacks that leads to the network collapse. In this paper, we proposed the 2-ACK scheme which is used for detecting the selfish nodes, eliminating them and choosing the other path for transmitting the data. After choosing the other path for transmitting the data there is a huge routing overhead is generated. So, we use Novel Routing algorithm which helps in decreasing the routing overhead and makes the network stable. In MANETs, Novel routing algorithm will also check the confidentiality of data message.**

Keywords **- Mobile Ad hoc Networks, Routing Misbehaviour, Packet Dropping Attack, Selfish, Malicious.**

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 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. Depending on its application, the formation of a MANET might vary from a small, fixed network that is highly power-inhibited to large scale, mobile, dynamic network. Packet loss is a common phenomenon due to this changing topology. Any wireless network consists of a lot of nodes that interact with each other exchanging information continuously. As these nodes have the flexibility of moving from one place to other, there may be cases where a particular node is a receiver for a particular packet, moves away from the range of sender. However the sender is not aware of this scenario and it might still keep on sending packets thus leading to data packet loss. The other case is more interesting, whenever communication takes place between any two nodes there are a lot of nodes involved in this communication process and acting as mediators. All these nodes consent to forward packets during the actual communication process but one of them actually turns selfish during transferring the data, this selfish/malicious node keeps on dropping data-packets as when received instead of forwarding it to the next hop in the communication process. The behaviour of selfishness results in packet loss and also the source is unaware of such misbehaving node in the path towards the destination. And there is no such mechanism to detect this misbehaving node.

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.

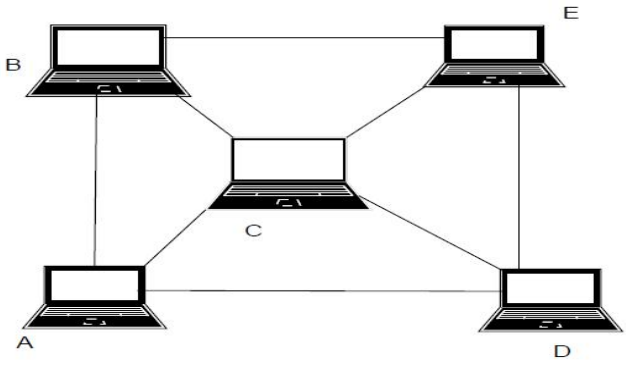


Fig. 1 Mobile Ad hoc networks

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. Routing as compared to wired networks is different in wireless networks. The traditional routing protocols fail to serve wireless networks, because these protocols put a lot of additional burden or computational overheads on mobile computers exhibit variable characteristics that do not meet the requirements of ad hoc networks.

There are two types of MANET:

1. **Open MANET**: An open MANET comprises of different users, having different goals, sharing their resources to achieve global connectivity.
2. **Closed MANET**: In closed MANET where the nodes are all controlled by a common authority, have the same goals, and work toward the benefit of the group as a whole.

Open environment of a MANET may lead to misbehaving nodes. Misbehaving nodes come into existence in a network due to several reasons:

- Mobile hosts lack adequate physical protection due to the open communication medium making them prone to be captured and compromised
- Usually mobile hosts are resource constrained computing devices.

A. Problem for Packet Dropping

In general, a packet can be dropped at either MAC or network layers due to the following reasons:

- The size of packet's transmission buffer at MAC level is limited; therefore whenever the buffer is full any new packet arriving from higher layers will be dropped (buffer overflow).
- IEEE 802.11 protocol's [1] rules: a data packet is dropped if its re-transmission attempts or the one of its corresponding RTS (Request To Send) frame has reached the maximum allowed number, owing to node's movement or collision.
- A data packet may be dropped or lost if it is corrupted during transmission due to some phenomenon specific to radio transmissions such as interference, hidden nodes and high-bit error rate.

In addition to these causes, a selfish node may refuse to relay a packet aiming to economize its energetic resources in order to extend its life-time or simply because its battery power is drained. Moreover a malicious node involved in a routing path may intentionally drop the packets at network layer in order to provoke a collapse in network performances. Furthermore, it can modify the IEEE 802.11 MAC protocol's parameters to provoke packet dropping. According to this analysis, packet dropping problem still open the door to new challenges in MANETs. For example, how can we recognize the reason leading a node to drop others' packets? In other words, how can we know the intention of a node to accuse it as malicious, selfish or legitimate?

The following **Fig.2** shows the scenario for packet dropping and mis-routing. Many packets are dropped due to the routing misbehaviour in MANETs.

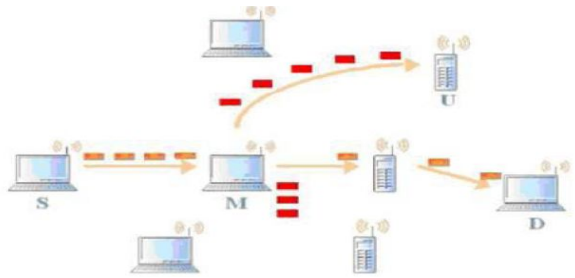


Fig. 2 Packet dropping and misrouting in MANETs

*B. **Selfish Node***

There are 3 types of Selfish nodes:

- Type 1 - Selfish Nodes (SN1): These types of nodes participate in route establishment but refuse to forward data packets (which are usually much larger than the routing control packets).
- Type 2 - Selfish Nodes (SN2): These nodes neither participate in the route establishment phase nor forward data packets. They only use their energy for transmissions of their own packets.
- Type 3 -Selfish Nodes (SN3): These nodes behave (or misbehave) differently based on their energy levels. When the energy lies between full energy E and a threshold T1, the node behaves properly. For an energy level between T1 and another lower threshold T2, it behaves like a node of type SN1. Finally, for an energy level lower than T2, it behaves like a node of type SN2. The relationship between T1, T2, and E is $T2 < T1 < E$. The existence of the SN2 type nodes is simply ignored by the routing protocol. Thus, these nodes do not pose a significant threat to the normal operation of the routing protocol, even though they may degrade network connectivity. On the other hand, SN1 and SN3 types of nodes are more dangerous to routing protocols [2].

These nodes support the flow of route discovery traffic but suspend the data flow, causing the routing protocol to restart the route discovery process or to select an alternative route if it is available. The recently selected routes may still include some of these SN1 type nodes and hence the new route will also fail. Until the source of traffic concludes that data cannot be transferred, this process will continue. In this work, we focus only on the detection and mitigation of SN1 type misbehaviour. SN3 type nodes will be detected, when they behave similar to the SN1 type nodes.

In order to detect misbehaving nodes, we propose a network-layer scheme called 2-ACK, which can be implemented as a simple add-on to any source routing protocol such as ALOHA. When a node forwards a data packet, the nodes routing agent verifies that the packet is received successfully by the node, that is two-hops away on the source route. This is done through the use of a particular type of acknowledgment packets, termed 2-ACK packets. 2-ACK packets have a very similar functionality as the ACK packets on the Medium Access Control (MAC) layer or the TCP layer. A node acknowledges the receipt of a data packet by sending back a two-hop 2-ACK packet along the active source route. If the data packet sender or forwarder does not receive a 2-ACK packet corresponding to a particular data packet that was sent out, the next-hop's forwarding link is claimed to be misbehaving and the forwarding route broken.

II. LITERATURE REVIEW

There is a lot's of work done on 2-ACK scheme, to mitigate the packet dropping attack many schemes are proposed such as Watchdog [3], Ex-Watchdog is proposed in [5], CONFIDANT [4], Two hop ACK [6], etc. We study & analyse the previous work related to our research, how 2-ACK scheme is actually worked, how they detect the selfish node and how its sends two-hop (3 nodes) acknowledgement packets in opposite direction.

The 2-ACK scheme is to detect malicious links and to mitigate their effects. This scheme is based on 2-ACK packet that is assigned a fixed route of two-hops in the opposite direction of the received data traffic path. In this scheme, each packet's sender maintains the following parameters:

(i). list of identifiers of data packets that have been sent out but have not been acknowledged yet,
(ii). a counter of the forwarded data packets, and
(iii). a counter of the packets missed.

According to the value of the acknowledgement ratio (Rack), only a fraction of data packets will be acknowledged in order to reduce the overhead. This technique overcomes some weaknesses of the Watchdog/path rather such as: power control transmission, ambiguous collisions and receiver collision. Thus it detects the selfish nodes, eliminate them and choose the other path for the data transmitting.

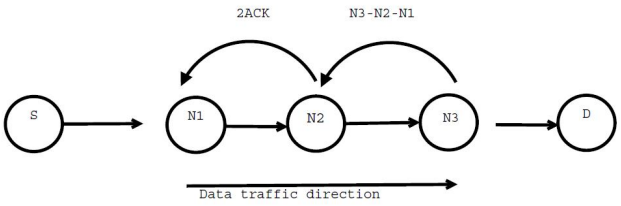


Fig. 3 2-ACK Scheme

III. PROBLEM DEFINITION AND DESCRIPTION

In MANETs packet dropping attack is the most destructive attack. The packet dropping is caused due to the selfish node or malicious node. To detect this selfish node lots of technique/scheme are used as discuss above. We are using 2-ACK scheme because it detects selfish node, eliminate them and choose the other path for transmitting the data. But this scheme had some limitations such as huge overhead is generated due to the extra acknowledgement packet sent and decision ambiguity, if the requested node refuse to send back an Acknowledgment [7]. Due to this limitation the efficiency of 2-ACK scheme decreases.

Our main aim is to improve the efficiency of 2-ACK scheme, reducing the routing overhead generated due to the extra acknowledgement packet sent and making the network stable.

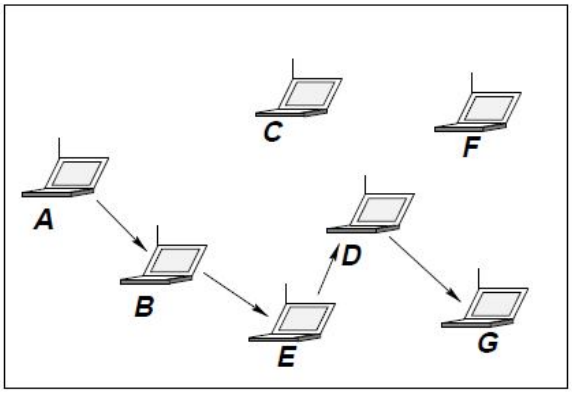
IV. TECHNIQUES TO IMPROVE THE EFFICIENCY OF 2-ACK SCHEME

To improve the efficiency and reducing the routing overhead generated due to the extra acknowledgement packet sent in 2-ACK scheme, we use Novel Routing Algorithm. This routing protocol is used to help to reduce the routing overhead and improve the efficiency.

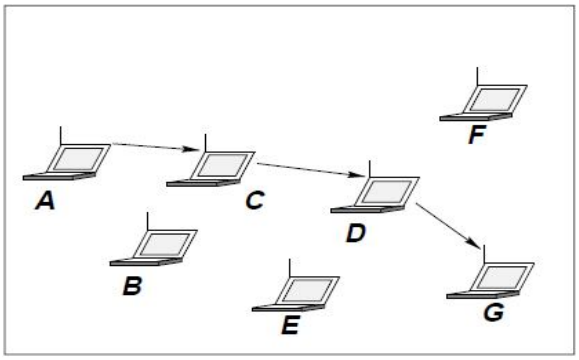
The Algorithm

Whenever a mobile node wants to join the MANET, it listens to the medium to find out a neighbour node *n*. Once a neighbour 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 [8].



(A)



(B)

Fig. 4 (A) Initial Route and (B) New Chosen Route

Fig. 4 shows first, 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.

V. CONCLUSIONS

From above research we conclude that a Novel routing protocol for MANETs that is based on mobile software agents modeled on ants. Ants are used to collect and disseminate information about the location of nodes in the network. This is a key aspect of the GPSAL algorithm that helps to accelerate route discovery. This algorithm is using the fixed hosts whenever possible to route packets. The combinations of these principles provide a better MANET routing algorithm. This algorithm increases the efficiency of 2-ACK scheme and reduces the routing overhead is generated in 2-ACK scheme.

REFERENCES

[1] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, ANSI/IEEE Std. 802.11, 1999.

[2] Conti M., Gregory E., and Muesli G, "Towards Reliable Forwarding for Ad Hoc Networks", Proc. Personal Wireless Comm. (PWC '03), pp. 790-804, Sept. 2003.

[3] S. Marti, T. J. Guile, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In Proc. 6th annual international conference on Mobile computing and networking (MOBICOM '00), Boston, Massachusetts, USA, August 2000.

[4] S. Buchegger and J. Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol," In Proc. 3rd ACM International Symposium on Mobile Ad Hoc Networking & computing (MOBIHOC'02), Lausanne, Switzerland, June 2002.

[5] N. Nasser and Y. Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks," In Proc. International Conference on Communication (ICC 07), Glasgow, June 2007.

[6] D. Djenouri and N. Badache, "New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks," In Proc. Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecurComm'05), Athens, Greece, September 2005.

[7] Soufiene Djahel, Farid Na¨ıt-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.

[8] Daniel Camara, Antonio A.F. Loureiro, "A Novel Routing Algorithm for Ad Hoc Networks," IEEE, 2000.