

# Detection of Misbehavior Link on the Basis of ACK System in MANET

Mr. Rushikesh Tupe<sup>1</sup> Mr. Shubham Tilekar<sup>2</sup> Mr. Nikhil Gaikwad<sup>3</sup> Mr. Swapnil Kadam<sup>4</sup>

<sup>1,2,3,4</sup>Department of Computer Engineering

<sup>1,2,3,4</sup>Trinity College of Engineering & Research, Pune, Maharashtra, India

**Abstract**— In mobile ad-hoc network there are individual mobile nodes which communicates through wireless link. The node does not share its resource but get advantage from other nodes are called misbehaving node. We use changing topologies with different nodes in mobile ad-hoc network. Because of misbehaving nodes network of performance affected. Misbehaving link in network, its sends two acknowledgement packets to the previous node from where the packets received. For minimizing the routing overhead we use modified acknowledgement scheme in that less amount of packets received. In modified two acknowledgement scheme we use DSR protocol for communication. Detecting misbehaving node in mobile ad-hoc network which shows host and routers connected by classic IP address is given in network. In mobile ad-hoc network nodes are connected either externally or internally. Mobile ad-hoc network interface connects routers. Classic IP address connects routers to nodes. In the network every node acts as basic node when it gets same configuration and properties from previous node. In mobile ad-hoc network node does not send data to next node therefore performance of network decreases. For finding misbehaving node in mobile ad-hoc network use three-hop technology which is more effective.

**Key words:** Dynamic Source Routing (DSR), Routing Misbehaviour, Misbehaviour Node, Network Security

## I. INTRODUCTION

A Mobile Ad Hoc Network is collection of mobile nodes. According to the movement of nodes, the topology of the network gets changed. MANET may vary from static network to dynamic network. There are two types of MANETs:

- 1) Closed MANET: all mobile nodes works with a common goal.
- 2) Open MANET: different nodes with different goals share their resources to ensure global connectivity.

A selfish nodes are those which may attempt to benefit from other nodes and refuse to share its own resources and their behavior is called selfishness or misbehavior. These nodes refuse to forward data packets for others in order to conserve its own energy.

MANET uses techniques like watchdog and path rater to detect and alleviate the effects of selfish nodes in MANET. Routing misbehavior can severely degrades the performance at the routing layer. Many nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. The 2ACKNOWLEDGEMENT scheme to mitigate adverse effects of misbehavior nodes.

In this scheme, when a node forward data packet to the next node, the destination node send two-hop acknowledgment called 2ACKNOWLEDGEMENT to indicate that the data packet has been received successfully. Such 2ACKNOWLEDGEMENT transmission takes place for only a fraction of data packets, but not for all. Such selective acknowledgment is intended to reduce the additional overhead caused by the

2ACKNOWLEDGEMENT scheme. Dynamic Source Routing protocol is used for evaluation of 2ACKNOWLEDGEMENT scheme.

## II. LITERATURE SURVEY

This paper proposes routing misbehavior detection in MANETs using 2ACKNOWLEDGEMENT scheme. Routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. Node misbehavior may exist due to the open structure and scarcely available battery-based energy.

In the existing system, a sender chooses a middle link to send some message to a destination, the middle link may not forward the packets to destination, it may be take long time to send packets or it may alter the contents of the packet. In MANETs, as there is no retransmission of packets once it is sent, care must be taken not to lose packets.

In this paper a technique, termed as 2ACKNOWLEDGEMENT scheme to detect and mitigate the effect of such routing misbehavior in MANETs environment. It is based on a simple 2-hop acknowledgment packet that is sent back by the receiver of the next-hop link. 2ACKNOWLEDGEMENT transmission takes place for only a fraction of data packets, but not for all. Such a selective acknowledgment is intended to reduce the additional routing overhead caused by the 2ACKNOWLEDGEMENT scheme. In this paper, some security aspects with 2ACKNOWLEDGEMENT to check confidentiality of the message by verifying the original hash code with the hash code generated at the destination. If 2ACKNOWLEDGEMENT is not received within the wait time or the hash code of the message is changed then the node to next hop link of sender is declared as the misbehaving link.

## III. PROBLEM DEFINITION

In the network while transferring the data from one node to another node through the middle node occurs some problems like:

- Data packets is not send from middle node to next node.
- It required more time to send data.
- Data may be alter while transmission.
- Our aim is used to detect misbehaving node and also checking the confidentiality of the message in the network.

## IV. SYSTEM REQUIREMENT

### A. Hardware Interaction:

There is no specific hardware required for interaction in our system. Our system simply requires package consisting of a basic hardware configuration: Intel Pentium II processor (Pentium III recommended), 128 MB of RAM (256 MB or more recommended), about 20 GB of hard disk space to

install Linux platform with Ns2 capability, color display and CD ROM.

### B. Software Interaction:

Any Linux platform supporting Ns2. The program has no other software requirements.

## V. SYSTEM MODEL

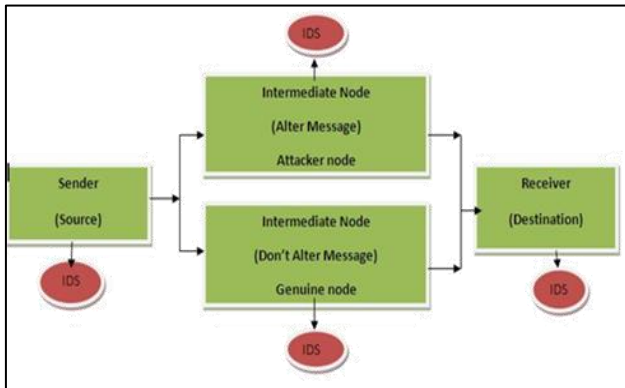


Fig. 1: System Model

### A. NODE 1:- (Source node)

- it take message and divides it in 48 bytes
- Sends it to receiver via middle node and get ack.
- "Counter packets" counter is incremented by 1 after each sending.
- If 2ACKNOWLEDGEMENT time less than wait time, "Counter misbehaving node" counter is increased by 1.
- Ratio of misbehaving node is threshold ratio
- If Counter of misbehaving node/Counter packets less than Ratio of misbehaving node, the link is working properly otherwise it is misbehaving.

### B. NODE 2:- (Middle node).

- Get packet from sender
- Replace/don't replace
- Get 2ACKNOWLEDGEMENT packet from receiver and sends 2 acknowledgements to sender.

### C. NODE 3:- (Destination node).

- Get message from middle node
- Find out destination name and hash code
- Decoding of hash code of destination and compares it with source's
- Sends 2ACKNOWLEDGEMENT to source via middle node. The task of this node is to get message from the middle node, find out destination name and hash code and decode it. Compare the hash code of source node and destination node for security purpose. Send 2ACKNOWLEDGEMENT to source through the middle node.

## VI. ALGORITHM

The triplet  $N1 \rightarrow N2 \rightarrow N3$  in Figure illustrate 2ACKNOWLEDGEMENT's processing. Take care about each codes are run on each of the sender/receiver of the 2ACKNOWLEDGEMENT packets. 2ACKNOWLEDGEMENT scheme

Packet at Sender Side (Node 3):

- 1) Step1: publish hn // Send authenticated element to N1
  - 2) Step2: Counter packets = 0, Counter acknowledgement = 0,  $i = n$ , Initialization at node N3
  - 3) Step 3: if (data packet received) then go to step 5.
  - 4) Step 4: Increase the counter packets
  - 5) Step 5: if (Counter acknowledgement = Counter packets less than Rack) then the data packet acknowledged needs to be prepare MAC with  $hi\{1$  prepare 2ACKNOWLEDGEMENT with ID, MAC,  $hi$ , Add authentication to 2ACKNOWLEDGEMENT packet
  - 6) Step 6: send 2ACKNOWLEDGEMENT
  - 7) Step 7: Increase the counter of acknowledged packets
- Packet at receiver side (Node 1):
- 8) Step 8: Parallel process 1 (receiving hn) While ( true) do.
  - 9) Step 9: if receive hn from the 2ACKNOWLEDGEMENT packet sender then Record  $hn, i n$
  - 10) Step 10: Parallel process 2 (receiving 2ACKNOWLEDGEMENT packets) while true do
  - 11) Step 11: if (data packet forwarded) then
  - 12) Step 12: stop
  - 13) Step 13: if (2ACKNOWLEDGEMENT packet received) then
  - 14) Step 14: stop
  - 15) Step 15: if (timeout event happens) then // 2ACKNOWLEDGEMENT packet for a data ID is not received
  - 16) Step 16 :End
  - 17) Step 17: if (Counter of misbehaving node = Counter packets greater than Ratio of misbehaving node) then the observation period expires
  - 18) Step 18: send link misbehavior report
  - 19) Step 19: Stop
  - 20) Step 20: Stop

## VII. CONCLUSION

MANETs are Mobile Ad Hoc Networks (MANETs) have been used for application in military and civilian communications. Such a network is highly dependent on the cooperation of all its members to perform networking functions. This makes selfish nodes. When such misbehaving nodes take part in the Route finding phase but refuse to forward the data packets, routing performance may be degraded severely. The 2ACKNOWLEDGEMENT scheme maintains up to 91% packet delivery ratio even when there are 40% misbehaving nodes in the MANETs nodes in MANETs.

## ACKNOWLEDGEMENT

The project on "Detection of Misbehavior link on the basis of ACK system in MANET" is a source of trending and immense information to us. We would glad to express our sincere gratitude to the "Trinity College of Engineering and Research department of Computer Technology for the guidance and most valuable support in the help for this project work. We acknowledge with a pleasant gratitude, the encouragement and inspiration received from our guide Prof.

Pavan Kulkarni, Head of the Department Prof. Dr. S. B. Chaudhari, Principal Dr. P. Dabeer and colleagues.

#### REFERENCES

- [1] N. Ramya ,Dr. S. Rathi,” 3rd International Conference on Advanced Computing and Communication Systems (ICACCS -2016), 978-1-4673-9206-8/16/\$31.00 ©2016 IEEE, Jan. 22 – 23, 2016
- [2] Hernandez-orallo Et Al, “Cocowa: A Collaborative Contact-based Watchdog For Detecting Selfish Nodes” IEEE Transactions On Mobile Computing, Vol. 14, No. 6, June 2015
- [3] E. Hern\_andez-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni, “Improving selfish node detection in MANETs using a collaborative watchdog,” IEEE Comm. Lett., vol. 16, no. 5, pp. 642–645, May 2012.
- [4] Rasika R. Mali, Sudhir T. Bagade, 2016 International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune,India 978-1-5090-1338-8/16/\$31.00 ©2016 IEEE, Dec 19-21, 2016
- [5] Arockia Rubi and Vairachilai, “A Survey on Intrusion Detection System in Mobile Adhoc Networks,” International Journal Of Computer Science And Mobile Computing, vol. 2, issue 12, pp. 389-393, December. 2013
- [6] Rasika Mali and Sudhir Bagade, “Techniques for Detection of Misbehaving Nodes in MANET: A Study,” International Journal of Scientific & Engineering Research, vol. 6, Issue 8, August 2015.
- [7] Hatware, A. Kathole, M. Bompilwar “Detection of Misbehaving Nodes in Ad Hoc Routing,” International Journal of Emerging Technology and Advanced Engineering, vol. 2, Feb. 2012.
- [8] Mangesh M Ghonge, Dr. V. M. Thakare, International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) Selfish Attack Detection in Mobile Ad hoc Networks,2016
- [9] Aishwarya Anand S Ukey, Meenu Chawla and Virendra Pal Singh, “I-2ACK: Preventing Routing Misbehavior in Mobile Ad hoc Networks”, International Journal of Computer Applications 62(12):34-39, January 2013.
- [10] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Transactions on Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.
- [11] Sunilkumar S. Manvia, Lokesh B. Bhajantrib, and Vittalkumar K. Vaggac, ‘ Routing Misbehavior Detection in MANETs’ Using 2ACKNOWLEDGEMENT, journal of telecommunication and information technology 4/2010.