RESEARCH ARTICLE OPEN ACCESS

Routing Misbehavior in MANETS

Prof. Priyadarshini Patil, Apeksha Joshi, Priyanka D, Shalini, Godavari
Department of Computer Science and Engineering
Godutai Engineering College for Women, Kalaburagi
Karnataka - India

ABSTRACT
Routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. However, due to the open structure and scarcely available battery-based energy, node misbehaviours may exist. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. In this paper, we propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme

Keywords:- Mobile Ad Hoc Networks (MANETs), routing misbehaviour, node misbehaviour, network security, Dynamic Source Routing (DSR)

I. INTRODUCTION

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 as routers. The operation of MANETs does not depend on pre existing infrastructure or base stations. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network.

There are two types of MANETs: closed and open [1]. In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be most important in a mobile environment. An individual mobile node may attempt to benefi3adest from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes, and their behaviour is termed selfishness or misbehaviour [2].One of the major sources of energy consumption in mobile nodes of MANETs is wireless transmission .A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy. Several techniques have been proposed to detect and alleviate the effects of such selfish nodes in MANETs . In [3], two techniques were introduced, namely watchdog and pathrater, to detect and mitigate the effects of the routing misbehavior, respectively. The watchdog technique identifies the misbehaving nodes by overhearing on the wireless medium. The pathrater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. The watchdog technique is based on passive overhearing. Unfortunately, it can only determine whether or not the next-hop node sends out the data packet. The reception status of the next-hop link's receiver is usually unknown to the observer. In order to mitigate the adverse effects of routing misbehavior, the misbehaving nodes need to be detected so that these nodes can be avoided by all well-behaved nodes.

II. PROBLEM IDENTIFICATION

In this, we focus on the following problem:

- Misbehaviour Detection and Mitigation [5]. In MANETs, routing misbehaviour can severely degrade the performance.

- A selfish node may refuse to forward data packets for other node in order to conserve its own energy.
- How do we detect such misbehaviour?
- How can we make such detection processes more efficient and accurate .

III. OBJECTIVES

Since our goal is to find that which node is misbehaving, to avoid such confusion while forwarding data packets from source to destination. and the destination should receive the information accurately.Our main intension is that the information should reach the destination node efficiently and reliably.

IV . METHODLOGY

The steps that are used in MANETS are: Sender node, Intermediate node, Destination node, Active, Passive and Node compromising

.

A. **Sender node (Source node):** The task of this node is to read the message and then divide the message into packet, send the packet to receiver through the intermediate node.

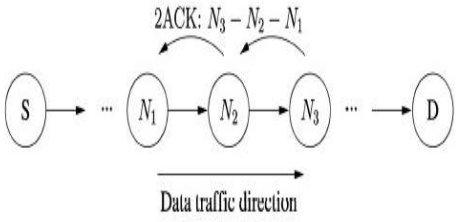
B. **Intermediate node:** The task of this node is to receive packet from sender, alter/don't alter the message and send to destination node.

C. **Destination node (Receiver node):** The task of this module is to receive message from the intermediate node, take out destination name and hash code and decode it.

D. **Active attack:** The active attack will change the IP address of the nodes and perform the attack. It may alter or do not alter the message. It disturb the operation of the network.

E. **Passive attack:** The passive attack will change the node has its destination node and send the information. It will not disturb the operation of the network.

F. **Node compromising:** The node compromising will change the digital signature of the node. Only the authenticated user can access the information by decrypting the message.



V RESULT ANALYSIS

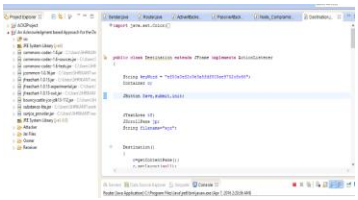


Fig a : Modules

A) SENDER

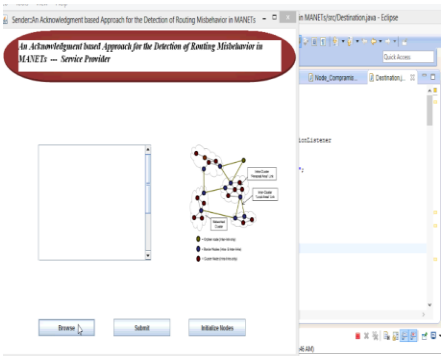


Fig 1 : Sender

B) ROUTING TABLE

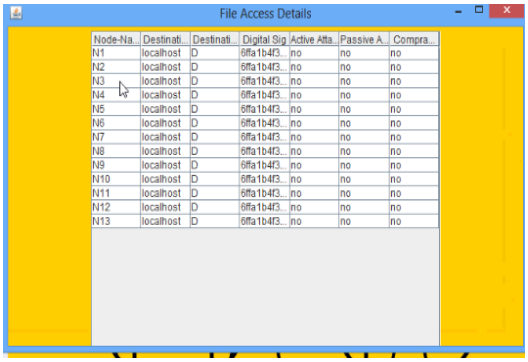


Fig 2:Routing table

C) ROUTING PATH

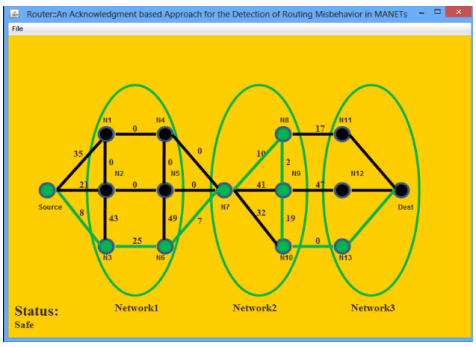


Fig 3 :Routing path

D) ACTIVE ATTACK

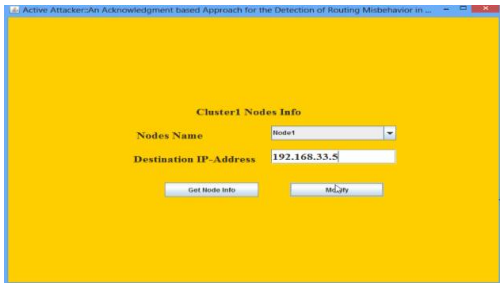


Fig 4:Active attack

E) ACTIVE ATTACK

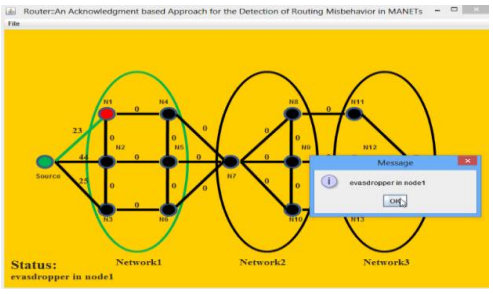


Fig 5:Active attack in cluster 1

F) ACTIVE ATTACK IN ROUTING TABLE

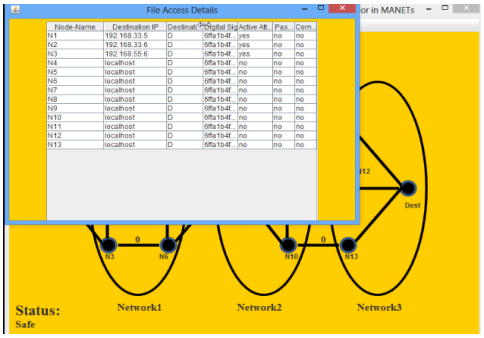


Fig 6: Active attack in routng table

G) PASSIVE ATTACK

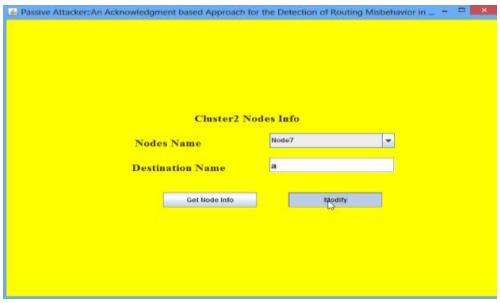


Fig 7 : Passive attack

H) PASSIVE ATTACK

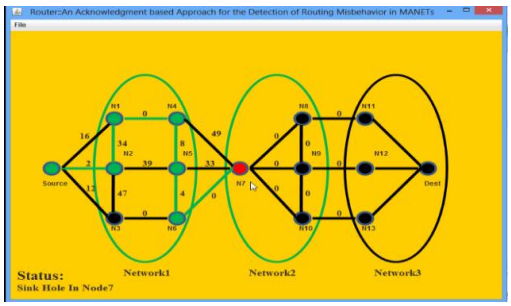


Fig 8 : Passive attack in cluster 2

I) PASSIVE ATTACK IN ROUTING TABLE

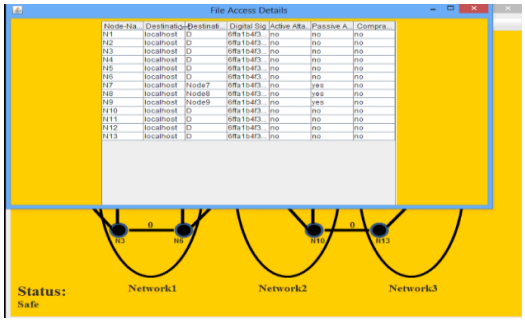


Fig 9: Passive attack in routing table

J) NODE COMPROMISING

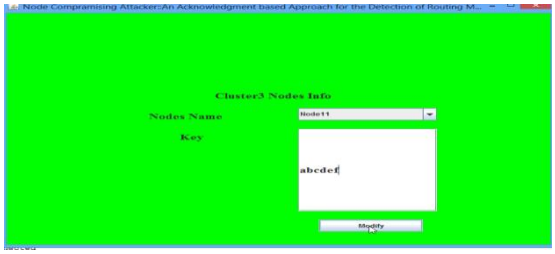


Fig 10: Node compromising

K) NODE COMPROMISING

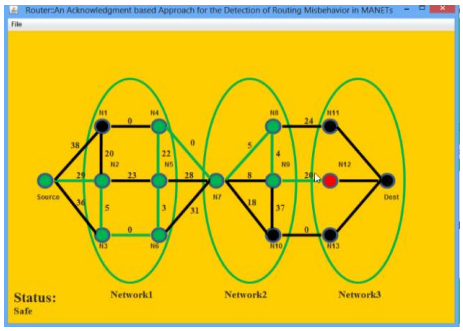


Fig 11 : Node compromising in cluster in 3

L) NODE COMPROMISING IN ROUTINH TABLE

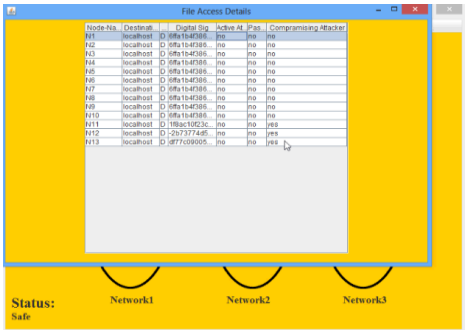


Fig 12 :Node compromising in routing table

VI. CONCLUSIONS

In MANETS we have investigated the performance degradation by selfish nodes. We have proposed and evaluated a technique termed has 2ACK scheme to dectect and mitigate the effect of routing misbehavior. Our main outcome is that we have been successfully avoided the misbehaving of nodes using 2ACK scheme.

REFERENCES

[1] H. Miranda and L. Rodrigues, "Preventing Selfishness in Open Mobile Ad Hoc Networks,"Proc. Seventh CaberNet Radicals Workshop, Oct. 2002.

[2] L.M. Feeney and M. Nilsson, "Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment," Proc. IEEE INFOCOM, 2001.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Techniques used in Mobile Ad Hoc Networks," Proc. MobiCom, Aug. 2000.

[4] D. Johnson, D. Maltz, Y.C. Hu, and J. Jetcheva, "The Dynamic Source Routing Protocol forMobile Ad Hoc Networks (DSR)," Internet draft, Feb. 2002.

[5] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom, Aug. 2000.

[6] Wang G Attebury, B Ramamurthy, "A survey of security issues in wireless sensor Networks,"2006-digital commons.uml.edu.

[7] A Manjeshwar, Q A Zeng , "An Analytical Mode for Information Retrieval in Wireless Sensor Networks

Using Enhanced APTEEN Protocol," 2002-IEEEXplore.IEEE.org

[8] R Yasmeen,E Ritter,G Wang, "An Authentication Framework for Wireless Sensor Network using Identity Based signatures,"computer and information 2010

[9] Harsh kupwade patil, Stephen A, szy genda "Secure Routing Protocol For Cluster-based Wireless Sensor Network",2012

[10] A. Sabri, Bandy Opadhyay cited by 1830,Heinzelman cited-13067, "Securtiy Model For Hierarchical Clustered Wireless Network",2014