ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Detection of Misbehavior Nodes in Manets Using 2ACK Method

Bhagyashree S. Madan [1], Prof. R. K. Krishna [2]

[1] Computer Science & Engineering, Rajiv Gandhi College of Engineering Research & Technology, Chandrapur, India

[2] Department of Electronics Engineering, Rajiv Gandhi College of Engineering Research & Technology, Chandrapur, India

bhagyashreemadan@yahoo.in

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 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. The nodes which drop the information to send forward considered as a selfish Node. Specifically, nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. To detect such misbehavior and more efficient detection process, the 2ACK technique is analyzed. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. Thus it detects the misbehaving nodes, eliminate them and choose the other path for transmitting the data. The main aim of this application is to detect the routing misbehavior in Manets that occurs due to the presence of selfish node. The input to the system will be the number of nodes with data transmission between them. The output of the system will involve detecting the misbehaving link and misbehaving node due to which the packet loss occurs.

Keywords: Mobile Ad hoc Networks (MANETs), misbehaving path, misbehaving nodes, packet loss, Route Discovery.

Introduction

MANETs are formed by a group of nodes that can transmit and receive data and also relay data among themselves. Communication between nodes is made over wireless links. A pair of nodes can establish a wireless link among themselves only if they are within transmission range of each other. An important feature of ad hoc networks is that routes between two hosts may consist of hops through other hosts in the network.

The source node will be able to choose an appropriate route to send its data. The 2ACK scheme is a network-layer technique to detect misbehaving links and to mitigate their effects. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

Selfish Nodes: An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish nodes or misbehaving nodes and their behavior is termed as selfishness or misbehavior. One of the major sources of energy consumption in the mobile nodes of MANET is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

The nodes of a MANET are actually mobile routers that build up routes dynamically. These routers can move randomly and insert themselves automatically into dynamic wireless topologies. They perform packet forwarding using the current routing information. A path form the source to the destination, that is, a route, can be established through well-known routing protocols such as the ad hoc on-demand distance vector routing (AODV), dynamic source routing (DSR). Selfish and malicious nodes take advantage of MANET idiosyncrasies to misbehave, or attack.

Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

broadly classified into two categories: credit-based schemes and reputation-based schemes.

A.Credit Based Schemes:
The idea of credit-based schemes is to provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes.

B.Reputation Based Schemes:
In reputation based schemes, network nodes collectively detect and declare the misbehavior of a suspicious node. Such a declaration is then propagated throughout the network so that the misbehaving node will be cut off from the rest of the network.
Routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. 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.

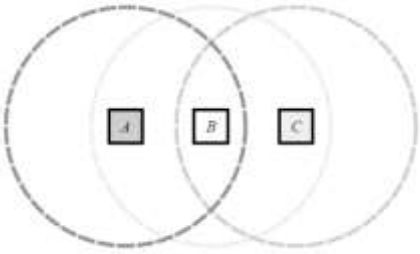

Fig1: A simple adhoc network of three wireless mobile host

C. Routing in MANETs:
Routing in ad hoc networks is different compared to normal wired networks. For instance, any routing scheme in a dynamic environment such as ad hoc networks must consider that the topology of the network can vary while the packet is being routed and that the quality of wireless links is highly variable. In wired networks, link failure is not frequent since the network structure is mostly static. Therefore, routes in MANET must be calculated much more frequently in order to keep up the same response level of wired networks. Routing schemes in MANET are classified in four major groups, namely, flooding, proactive routing, reactive routing, and hybrid routing.

In pro-active routing (table-driven), valid routes are maintained to every node all the time. Updates are propagated throughout the network when a change in the network topology occurs. Proactive routing is only appropriate for small networks because as networks grow in size the overhead increases.

In reactive routing (on-demand) the route evaluation is done only when it is necessary. When a node needs to find a route to another destiny node it must begin a discovery process to find one that is appropriate. Paths are maintained only until they are needed.

Hybrid routing provides routing through the implementation of a hierarchical approach. In a hierarchical approach the network is organized into subsets of nodes, known as clusters. This topology organization reduces network traffic because a node only needs to have knowledge of the routing information within its cluster and not of the entire network.

D. End-to-End Acknowledgment Schemes
There are several schemes that use end-to-end acknowledgments (ACKs) to detect routing misbehavior or malicious nodes in wireless networks. In the TCP protocol, end-to-end acknowledgment is employed. Such acknowledgments are sent by the end-receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. The Selective Acknowledgment (SACK) technique is used to acknowledge out-of-order data blocks.

The 2ACK technique differs from the ACK and the SACK schemes in the TCP protocol:
The 2ACK scheme tries to detect those misbehaving nodes which have agreed to forward data packets for the source node but refuse to do so when data packets arrive. TCP, on the other hand, uses ACK and SACK to measure the usefulness of the current route and to take appropriate action.

E.The TWOACK and S-TWOACK Schemes
TWOACK is an early version of the 2ACK scheme. There are several schemes that use end-to-end acknowledgments (ACKs) to detect routing misbehavior or malicious nodes in wireless networks. In the TCP protocol, end-to-end acknowledgment is employed. Such acknowledgments are sent by the end-receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. The Selective Acknowledgment (SACK)

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

technique is used to acknowledge out-of-order data blocks.
The 2ACK technique differs from the ACK and the SACK schemes in the TCP protocol in the following manner: The 2ACK scheme tries to detect those misbehaving nodes which have agreed to forward data packets for the source node but refuse to do so when data packets 2ACK scheme.

Literature review

David B. Johnson and David A. Maltz present a protocol for routing in ad hoc networks that uses dynamic source routing. First, unlike conventional routing protocols, our protocol uses no periodic routing advertisement messages, thereby reducing network bandwidth overhead; particularly during periods when little or no significant host movement is taking place. This paper has presented a protocol for routing packets between wireless mobile hosts in an ad hoc network. The protocol presented here is explicitly designed for use in the wireless environment of an ad hoc network. There are no periodic router advertisements in the protocol. Instead, when a host needs a route to another host, it dynamically determines one based on cached information and on the results of a route discovery protocol. Based on results from a packet-level simulation of mobile hosts operating in an ad hoc network, the protocol performs well over a variety of environmental conditions such as host density and movement rates [1].

Elizabeth Royer and C-K Toh provide a classification of these schemes according to the routing strategy (i.e., table-driven and on-demand).Challenges facing ad hoc mobile wireless networks. On-Demand Distance Vector (AODV) routing protocol described builds on the DSDV algorithm. Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. [6].

Buchegger S. and Le Boudec J.-Y Presents the CONFIDANT protocol works as an extension to a reactive source-routing protocol for mobile ad-hoc networks. Dynamic Source Routing is a protocol developed for routing in mobile ad-hoc networks. This paper recognizes the special requirements of mobile ad-hoc network in terms of cooperation, robustness, and fairness. Reputation systems are used in some online auctioning systems. They provide a means of obtaining a quality rating of participants of transactions by having both the buyer and the seller give each other feedback on how their activities were perceived and evaluated. [4].

Quansheng Guan, F. Richard Yu, Shengming Jiang In this paper, they focus on authentication and topology control issues. A joint authentication and topology control (JATC) scheme is proposed to improve the throughput. Simulation results have been presented to show that JATC works well in MANETs. The ultimate objective of JATC is to optimize the joint authentication and topology configuration to maximize the per node aggregate throughput capacity, i.e., the sum of all the throughput of links associated with the node. [7].

Erman Ayday, Faramarz Fekri presents in conventional Mobile Ad hoc Networks (MANETs), the existence of end-to-end paths via contemporaneous links is assumed in spite of node mobility. Define the packet delivery ratio as the ratio of the number of legitimate packets received by their destinations to the number of legitimate packets transmitted by their sources. [8].

Balakrishnan K., Deng J., and Varshney P. K present two network-layer acknowledgment-based schemes, termed the TWOACK and the S-TWOACK schemes. Selfishness, which is notably different from malicious behavior. Selfish nodes use the network for their own communication, but simply refuse to cooperate in forwarding packets for other nodes in order to save battery power. [3].

Proposed model

The 2ACK technique differs from the ACK and the SACK schemes in the TCP protocol:
The 2ACK scheme tries to detect those misbehaving nodes which have agreed to forward data packets for the source node but refuse to do so when data packets arrive. TCP, on the other hand, uses ACK and SACK to measure the usefulness of the current route and to take appropriate action.

The proposed work (2ACK with confidentiality) is as follows.

- If the 2ACK time is less than the wait time and the original message contents are not altered at the intermediate node then, a message is given to sender that the link is working properly.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

- If the 2ACK time is more than the wait time and the original message contents are not altered at the intermediate node, then a message is given to sender that the link is misbehaving.
- If the 2ACK time is more than the wait time and the original message contents are altered at the intermediate node, then message is given to sender that the link is misbehaving and confidentiality is lost.
- If the 2ACK time is less than the wait time and the original message contents are altered at the intermediate node then, a message is given to sender that the link is working properly and confidentiality is lost.

When Node 1 wishes to send the data packets to node 3, so in this process node 2 considered as an intermediate node. In figure 4, the path from node2 to node3 is seems to be misbehaving. After the proper timing sender get message the link is misbehaving.

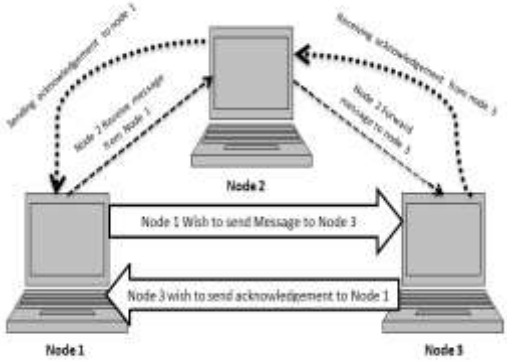

Fig 2: System model

.

In the existing system, there is a possibility that when a sender chooses an intermediate link to send some message to destination, the intermediate link may give problems such as the intermediate node may not forward the packets to destination, it may take very long time to send packets or it may modify the contents of the packet Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, we have focused on the problem of detecting misbehaving links instead of misbehaving nodes using 2ACK scheme.

For this first we have to implement a model connecting node in adhoc network and each node in an adhoc networking act as a client and act as destination. We are implementing here source and destination that source sending message to other node in a range and if the message received by other node, it sends back an acknowledgement to the source. When source get an acknowledgement source have conform that message is received by destination. The result is that this link will be tagged. Our approach is used to discuss the significantly simplification of the routing detection mechanism and also checking the confidentiality of the message in MANETs environment.

Authenticating the 2ACK Packets

When the 2ACK packets are forwarded by an intermediate node without proper protection, a misbehaving node *N*2 can simply fabricate 2ACK packets and claim that they were sent by node *N*3. Therefore, an authentication technique is needed in order to protect 2ACK packets from being forged. To stop *N*2 from forging the 2ACK packets is to use the digital signature algorithm.

A digital signature is a small number of extra bits of information attached by node *N*3. The signature is unique and usually computationally impossible to forge unless the security key of node *N*3 is disclosed. Furthermore, the signature may be used to assure the integrity of the transmitted data, i.e., any changes on the signed information will be detected. Typically, the digital signature is implemented relying on asymmetric cryptography. But, such asymmetric operations are too expensive for the mobile nodes in MANETs which are usually resource constrained.

Advantages of 2ACK scheme

It solves the problems of ambiguous collisions, receiver collisions, and limited transmission power:

A. Ambiguous Collisions: Ambiguous collisions may occur at node *N*1. When a well-behaved node *N*2 forwards the data packet toward *N*3, it is possible that *N*1 cannot overhear the transmission due to another concurrent transmission in *N*1's neighborhood. The 2ACK technique solves this problem by requiring *N*3 to send a 2ACK packet explicitly.

B. Receiver Collisions: Receiver collisions take place in the overhearing techniques when *N*1 overhears the data packet being forwarded by *N*2, but *N*3 fails to receive the packet due to collisions in its neighborhood. A misbehaving *N*2 will not retransmit the data packet, which costs extra energy. Again, the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

2ACK technique overcomes this problem due to the explicit 2ACK packets.

C. Limited Transmission Power: A misbehaving *N*2 may maneuver its transmission power such that *N*1 can overhear its transmission but *N*3 cannot. This problem is similar to the Receiver Collisions problem. It becomes a threat only when the distance between *N*1 and *N*2 is less than that between *N*2 and *N*3. The 2ACK scheme is immune to limited transmission power problem.

D. Limited Overhearing Range: A well-behaved *N*2 may use low transmission power to send data toward *N*3. Due to *N*1's limited overhearing range, it will not overhear the transmission successfully and will thus infer that *N*2 is misbehaving, causing a false alarm. Both this problem and the limited transmission power problem are caused by the potential asymmetry of communication links. The 2ACK scheme is immune to the limited overhearing range issue.

Experimental results

Node 1 Wishes to send packets to node 3. Message forwarded from node1 but not receive by node 3 because the link is misbehaving. After Some time node1 get message that the path is misbehaving.

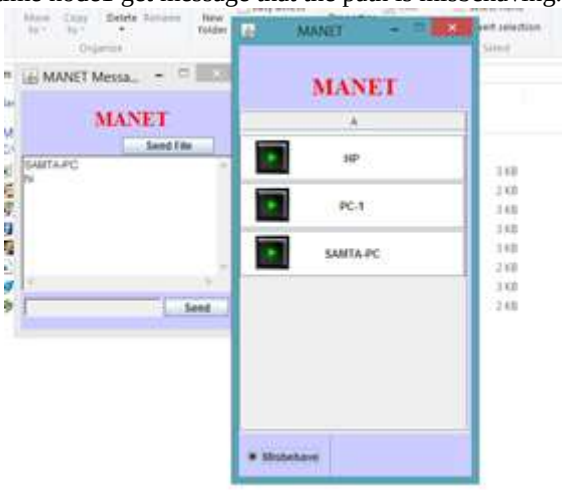

Fig 3: Selecting Nodes which are in range

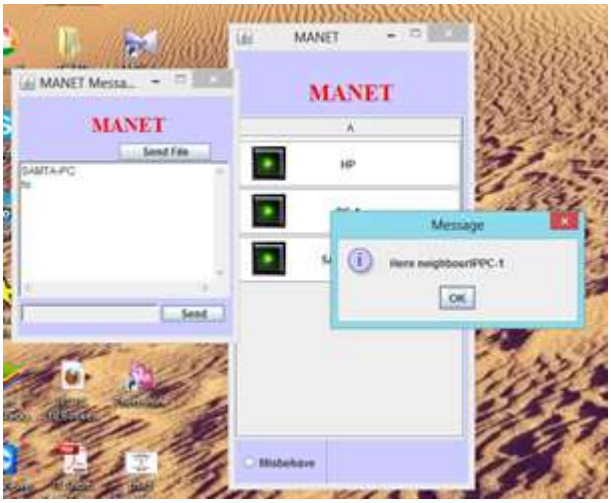

Fig 4- Detecting the nighbour node

Fig 5: Sending File

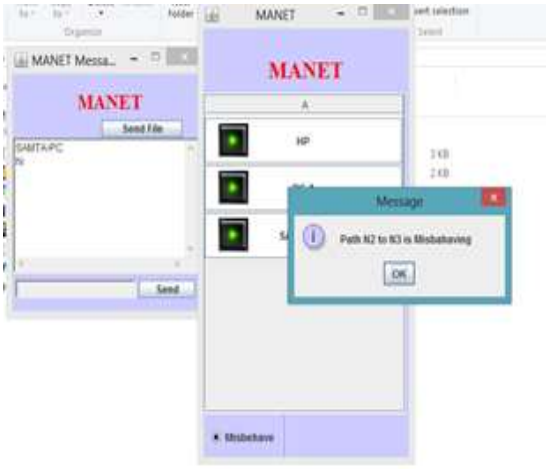

Fig 6: Detecting the path is misbehaving

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Fig 7- Detecting the misbehaviour node

Conclusion

When selfish misbehaving nodes participate in the Route Discovery but refuse to forward the data packets, routing performance may be degraded severely. The 2ACK scheme maintains packet delivery ratio even when there are misbehaving nodes in the MANET. The 2ACK scheme detects misbehaving node and reduces the number of ACKs. For applying directly 2ACK Scheme on number of nodes, it is necessary to connect nodes in adhoc network and implement sending message and receiving acknowledgment between the nodes and after that applying 2ACK scheme for detecting misbehaving link and in this and then detecting the misbehavior node.

References

1. *David B. Johnson, David A.Maltz Computer Science Department Carnegie Mellon University 5000 Forbes Avenue Pittsburgh "Dynamic Source Routing in Ad Hoc Wireless Networks".Tomasz Imielinski and Hank Korth, Kluwer Academic Publishers, 1996.*
2. *Baker M, Giuli T., Lai K. and Marti S., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom, pp. 255-265, Aug. 2000.*
3. *Balakrishnan K., Deng J., and Varshney P. K., "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), pp.2137-2142 Mar. 2005.*
4. *Buchegger S. and Le Boudec J.-Y., "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, pp. 226-236, June 2002.*
5. *D. Johnson, D. Maltz, Y.C. Hu, and J. Jetcheva. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)" in 10th IEEE International Conference, 27-30 Aug 2002 Year of Publication: 2002, ICON 2002.*
6. *Elizabeth Royer and C-K Toh "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks". IEEE Personal Communications Magazine,pages 46-55, April 1999.*
7. *Quansheng Guan, F. Richard Yu, Shengming Jiang "Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks with Cooperative Communications" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. VOL. 61, NO. 6, JULY 2012.*
8. *Erman Ayday, Faramarz Fekri on "An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO.9, SEPTEMBER 2012.*
9. *Bhagyashree S. Madan and Prof.R.K.Krishna, Rajiv Gandhi College of Engineering__Rajiv Gandhi College of Engineering, Research & Technology,Chandrapur."Misbehavior of Nodes in MANETs Using ACK Scheme" has International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 11, November – 2013. ISSN: 2278-0181*
10. *Bhagyashree S. Madan and Prof.R.K.Krishna, Rajiv Gandhi College of Engineering__Rajiv Gandhi College of Engineering, Research & Technology, Chandrapur. "Working of Acknowledgements for Detecting Misbehavior Nodes in MANETs" paper in National Conference on Research Trends in Electronics, Computer Science & Information Technology.*