Misbehavior of Nodes in MANETS using Ack Scheme

Bhagyashree S. Madan[#], Prof. R. K. Krishna[*]
Department of Computer Science & Engineering[#]
Department of Electronics Engineering[*]
Rajiv Gandhi College of Engineering, Research & Technology, Chandrapur
Maharashtra, 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 as routers. 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. 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. Thus it detects the misbehaving nodes, eliminate them and choose the other path for transmitting the data. The watchdog detection mechanism has a very low overhead. Unfortunately, the watchdog technique suffers from several problems such as ambiguous collisions, receiver collisions, and limited transmission power. The main issue is that the event of successful packet reception can only be accurately determined at the receiver of the next-hop link, but the watchdog technique only monitors the transmission from the sender of the next-hop link.

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

1. 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 MANETs 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 MANET.

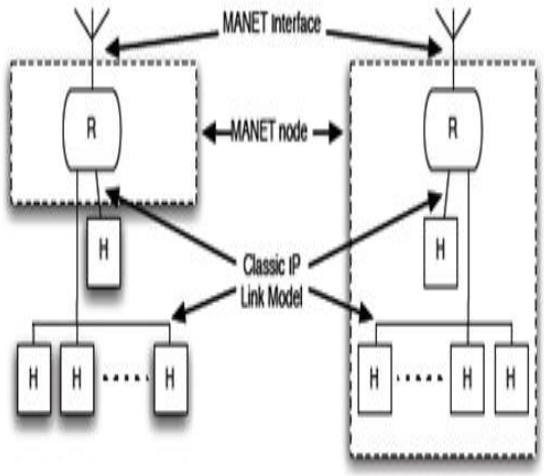

Fig 1: MANET node model

1.1 There are two types of MANETs:

a) Closed MANET:

In a closed MANET, all mobile nodes cooperate with each other towards a common goal, such as emergency search/rescue or military and law enforcement operations.

b) Open MANET

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 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 MANETs is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

This paper is organized as follows; Section 2 introduces the basic acknowledgements schemes; Section 3 gives the literature review; Section 4 discusses our proposed methods; Section 5 gives the conclusion to the problem.

1.2 MANET ROUTING

To find and maintain routes between dynamic topology with possibly uni-directional links, using minimum resources. The use of conventional routing protocols in a dynamic network is not possible because they place a heavy burden on mobile computers and they present convergence characteristics that do not suit well enough the needs of dynamic networks [5]. For Example, any routing scheme in a dynamic environment for instance ad hoc networks must consider that the topology of the network can change while the packet is being routed and that the quality of wireless links is highly variable. The network structure is mostly static in wired networks that are why link failure is not frequent. Therefore, routes in MANET must be calculated much more frequently in order to have the same response level of wired networks. Routing schemes in MANET are classified in four major groups, namely, proactive routing, flooding, reactive routing, and hybrid routing.

1.3 MISBEHAVIOUR OF NODES IN MANET

Ad hoc networks increase total network throughput by using all available nodes for forwarding and routing. Therefore, the more nodes that take part in packet routing, the greater is the overall bandwidth, the shorter is the routing paths, and the smaller the possibility of a network partition. But, a node may misbehave by agreeing to forward packets and then failing to do so, because it is selfish, overloaded, broken, or malicious

2. Acknowledgement Schemes

2.1 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. That is, congestion control is based on the reception of the ACK and the SACK packets.

The *secure traceroute*protocols used to identify malicious routers that draw traffic toward themselves but fail to correctly forward the traffic. The normal traceroute protocol allows the sender to simply send packets with increasing Time-To-Live (TTL) values and wait for a warning message from the router at which time the packet's TTL value expires. The secure trace route protocol authenticates the trace route packets and disguises them as regular data packets.

To secure the trace route scheme, binary search is initiated on faulty routes. Asymptotically, log(n) probes are needed to identify a faulty link on a faulty n-hop route. This technique only works with static misbehaviors and needs to disguise the probing messages as regular routing control packets. Once a link is identified as faulty, the link weight is increased so that future link selections will avoid this link.

2.2 The TWOACK Scheme

The TWOACK scheme can be implemented on top of any source routing protocol such as DSR. This follows from the fact that a TWOACK packet derives its route from the source route established for the corresponding data packet. The TWOACK scheme uses a special type of acknowledgment packets called TWOACK packets, which are assigned a fixed route of two hops (or three nodes) in the direction opposite to that of data packets. Note that the ACK packets at the TCP layer have a similar effect as our TWOACK packets do. The main differences are the following: First, ACK packets in TCP are used for the purpose of flow-control and reliable end-to-end communication, while selfishness is more a problem that should be solved by the underlying IP layer. In the absence of a lower layer acknowledgment scheme, the source and other intermediate nodes have no way of finding out which of the downstream nodes is misbehaving. It will be inefficient to conclude that the entire route is misbehaving when indeed there is only one misbehaving node.

2.3 The S-TWOACK Scheme

The TWOACK scheme described above gives rise to two hops of TWOACK packets for every hop of data packet being forwarded. Considering that each TWOACK packet is a unique entity and has to contend for the medium just like any other packet, the TWOACK packets may contribute to the traffic congestion on the routing path. Therefore, we further propose the S-TWOACK (Selective-TWOACK) scheme, a derivative of the TWOACK scheme, to reduce this extra traffic due to TWOACK packets. In the S-TWOACK scheme, instead of sending back a TWOACK packet every time when a data packet is received, a node waits until a certain number of data packets (through the same triplet) arrive. The node then sends back one TWOACK packet acknowledging multiple data packets that have been received so far. The S-TWOACK scheme has three parameters: *timeout*, *timeout Last Sent* and *maximum IDs Carried*. While *timeout* has the same usage as that in the TWOACK scheme, the use of the other two parameters can be explained as below: when the number of data packets received at *N*3 reaches *maximumIDs Carried* or the duration since sending the TWOACK packet last time is larger than *timeout Last Sent*, a TWOACK packet will be sent. Note that, although the S-TWOACK scheme is expected to provide a significant reduction of routing overhead, it comes with a cost: the problem of false-alarms due to genuine TWOACK packets lost is more noticeable.

The Selective TWOACK (S-TWOACK) scheme is also different from 2ACK. Mainly, each TWOACK packet in the S-TWOACK scheme acknowledges the receipt of a number of data packets, but a 2ACK packet in the 2ACK scheme only acknowledges one data packet. With such a subtle change, the 2ACK scheme has easier control over the trade-off between the performance of the network and the cost as compared to the S-TWOACK scheme.

2.4 2ACK Scheme

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. Thus it detects the misbehaving nodes, eliminate them and choose the other path for transmitting the data. The watchdog detection mechanism has a very low overhead. Unfortunately, the watchdog technique suffers from several problems such as ambiguous collisions, receiver collisions, and limited transmission power. The main issue is that the event of successful packet reception can only be accurately determine at the receiver of the next-hop link, but the watchdog technique only monitors the transmission from the sender of the next-hop link.

3. Literature Review

Tomasz Imielinski and Hank Korth, Kluwer presents 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 Tohprovide 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 objective of topology control is achieved by adjusting some controllable parameters that affect link status, such as transmission power, antenna direction, channel assignment, cooperative level, and transmission manners. 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].

ErmanAyday, FaramarzFekripresents in conventional Mobile Ad hoc Networks (MANETs), the existence of end-to-end paths via contemporaneous links is assumed in spite of node mobility. The main goal for building a reputation system in MANETs is to protect the reactive routing protocol from attackers and increase the performance of the network. In this paper, they introduced a robust and efficient security mechanism for delay-tolerant networks. DTNs are characterized by intermittent contacts between nodes, leading to space time evolution of multihop paths (routes) for transmitting packets to the destination. An insider adversary drops legitimate packets it has received. This behavior of the malicious nodes has a serious impact on the data availability and the total latency of the network. Moreover, a malicious node may also generate its own flow to deliver to another (malicious) node via the legitimate nodes. As a result, bogus flows compete with legitimate traffic for the scarce network resources. The main goal for building a reputation system in MANETsis to protect the reactive routing protocol from attackers and increase the performance of the network 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. Two modules called watchdog and pathrater are implemented at each node, to detect and mitigate, respectively, routing misbehaviors in MANETs. In order to detect misbehaving nodes, we propose a network-layer scheme called TWOACK, which can be implemented as a simple add-on to any source routing protocol such as DSR The TWOACK scheme will not be affected by ambiguous collisions at the sender or the receiver. The underlying MAC layer ensures the reliable transmission of such TWOACK packets. Nodes operate in a promiscuous mode wherein, the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet or not. At the same time, it maintains a buffer of recently sent packets [3].

4. Proposed Model

The Motivation of this research work is to focus on the issues related with wireless adhoc networks which still remain unfocussed. 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. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behavior is termed selfishness or misbehavior. A selfish node may refuse to forward data packets for other nodes in order to

conserve its own energy. This misbehavior results into packet loss. Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, we focus on the problem of detecting misbehaving links instead of misbehaving nodes. In the next-hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet. Ad-hoc networks are suited for use in situations where an infrastructure is unavailable or to deploy one is not cost effective. The famous IEEE 802.11 or Wi-Fi protocol also supports an ad-hoc network system in the absence of a wireless access point. Another application example of a mobile adhoc network is Bluetooth, which is designed to support a personal area network by eliminating the need of wires between various devices, such as printers and personal digital assistants.

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. In MANETs, as there is no retransmission of packets once it is sent, hence care is to be taken that packets are not lost. 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. In the next-hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet. It will not be forwarded further. 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.

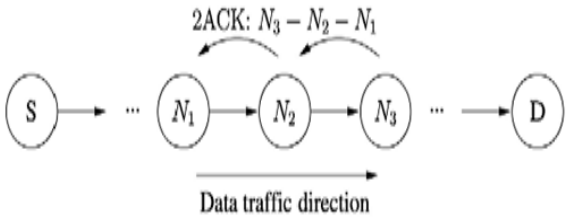

Fig. 2 ACK Scheme

4.1 CONFIDANT

The CONFIDANT protocol is designed as an extension to an on demand routing protocol, such as the DSR. CONFIDANT facilitates monitoring and reporting for a route establishment that avoids the misbehaving nodes. It is based on the assumption that the packets of misbehaving nodes are not forwarded by fair nodes. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. The CONFIDANT protocol works as an extension to a reactive source-routing protocol for mobile ad-hoc networks. For the simulation implementation, we have chosen Dynamic Source Routing (DSR) as the base protocol. In the following subsections we briefly describe what we need to know about DSR, describe the attacks we support, and specify how we want to thwart them. Observable attacks on forwarding and routing in mobile ad-hoc networks can be thwarted by the suggested CONFIDANT scheme of detection, alerting, and reaction. The CONFIDANT protocol is scalable in terms of the total number of nodes in a network and performs well even with a fraction of malicious nodes as high as 60%.

4.2 DYNAMIC SOURCE ROUTING

The *Dynamic Source Routing* protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. Network nodes (computers) cooperate to forward packets for each other to allow communication over multiple "hops" between nodes not directly within wireless transmission range of one another. As nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR routing protocol. Since the number or sequence of intermediate hops needed to reach any destination may change at any time, the resulting network topology may be quite rich and rapidly changing. The DSR protocol allows nodes to dynamically discover a *source route* across multiple network hops to any destination in the ad hoc network. Each data packet sent then carries in its header the complete, ordered list of nodes through which the packet must pass, allowing packet routing to be trivially loop-freely and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. By including this source route in the header of each data packet, other nodes forwarding or overhearing any of these packets may also easily cache this routing information for future use.

5. Conclusion

When selfish misbehaving nodes participate in the Route Discovery but refuse to forward the data packets, routing performance may be degraded severely. The 2ACKscheme maintains packet delivery ratio even when there are misbehaving nodes in the MANET. The 2ACK detects misbehaving node and reduces the number of ACKs. A 2ACK packet will assigned a fixed route of two hops (four nodes N1, N2, N3, N4), in the opposite direction of the data traffic route. The system will implement the 2ACK scheme which helps to detect misbehavior by 3 hop acknowledgement.

6. References

[1] David B. Johnson, David A.MaltzComputer 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] ErmanAyday, FaramarzFekri 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