National Conference on Emerging Trends in Computer, Electrical & Electronics (ETCEE-2015)
International Journal of Advance Engineering and Research Development (IJAERD)
e-ISSN: 2348 - 4470 , print-ISSN:2348-6406,Impact Factor:3.134

Study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks

Richa Sheth[1], Rashmi Agrawal[2]

[1,2]*Computer Department, Gujarat Technological University*
Address
[1]rmsheth1@gmail.com
[2]rashmi.agrawal@aits.edu.in

***Abstract*—A MANET(Mobile Ad hoc network) consists of mobile nodes connected through wireless links. MANETs are self-configuring networks without having fixed infrastructure. Each node has to rely on other nodes to forward its data packets. Mobile ad hoc networks can function properly only if participating nodes collaborate in routing and forwarding. Since most of the nodes are constrained by battery power and computing resource, few nodes may refrain to cooperate and do not forward packets destined for other nodes. This leads to degradation of the network performance. Selfish nodes do not consume any energy such as battery power, CPU power and bandwidth for retransmitting the data packets of other nodes and they reserve them for themselves. In this paper we give an overview of Credit based techniques and reputation based schemes used for detection of selfish nodes.**

***Keywords*—Mobile Ad hoc network(MANET), Dynamic source routing, Selfish nodes in MANET, Watchdog, Pathrater**

I. INTRODUCTION

A Mobile Ad-hoc Network consists of group of mobile devices communicating with each other through wireless medium. Here the network is established solely by MANET devices themselves without the need of any fixed infrastructure such as access point or base station. Each node in the network acts as host as well as router to forward packet to other nodes. MANETs have few special features such as wireless links for communication, dynamic topology, distributed operation, multi-hop routing ,limited bandwidth, battery lifetime etc. It is used in a wide range of applications such as military battlefield, rescue operations ,personal area networks and commercial sector .

MANETs have several operating constraints [2] such as limited battery charge per node, limited transmission range per node and limited bandwidth. Generally routes in MANETs are often multi-hop in nature. Power consumption in mobile ad hoc network is directly proportional to route length i.e. if route length is increased then power consumption is also increased to route a packet. A node consumes its battery power for each transmission and reception of data packet. Thus the more it will transmit or receive data packets ,more power will be consumed. Nodes forward packets for their peers in addition to their own, in other words, nodes are forced to spend their battery charge for receiving and transmitting packets that are not intended for them. Because of MANETs have the limited energy budget [2] for communication among mobile nodes, thus usage of the energy resources of a small set of nodes at the cost of others can have an adverse impact on the node lifetime as well as network lifetime.

MANET are basically of two types closed and open[8]. In case of closed MANET all mobile nodes cooperate with one other. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. Some mobile nodes may attempt to benefit from other nodes, but refrain from sharing its own resources with other nodes. Such nodes are called selfish or misbehaving nodes, and their behavior is termed selfish or misbehavior. One of the major sources of energy consumption in mobile nodes of MANET is wireless transmission.

Ad hoc network maximize the total network throughput by utilizing all available nodes for routing and forwarding. Therefore, the more nodes participate in packet routing, the greater the aggregate bandwidth, the shorter the possible routing paths, and the smaller the possibility of a network partition[9]. However, a node may misbehave by agreeing to forward packets and then failing to do so, because it is selfish, malicious, overloaded or broken. An overloaded node has insufficient CPU power, buffer space or available network bandwidth to forward the packets. A selfish node is unwilling to spend its battery power, CPU cycles, or available network bandwidth to forward packets destined for others, even though it expects others to forward packets on its behalf. A malicious node launches a denial of service attack by dropping packets. A broken node may have a software fault so it prevents from forwarding packets.

The rest of the paper is organized as follows. The second section describes about misbehaving nodes in MANET and the third section gives brief introduction to DSR protocol. The fourth section describes about various techniques used for detection and prevention of selfish nodes in MANET. The fifth section concludes the paper.

II. NODE MISBEHAVIOUR IN MANET

As there is no dedicated infrastructure or central coordination in MANET, the nodes have to cooperate with one another to form a working communication network. Communication

only works if nodes participate and forward other node's packets. On the other hand every node has to consider its limited resources(most notably its energy). So every node is motivated to contribute as little as possible of its own energy. Usually, it is expected that all nodes forward as needed, but other possibilities also work(e. g. only require forwarding as long as a node's battery level is high). In any way the MANET's protocols and policies imply a normative expectation on every participating node a) to behave according to agreed protocols and b) to forward a fair amount of other node's packets as needed. As long as all nodes adhere to this and cooperate, the MANET works effectively without any problem. One of the most important issues in designing MANET protocols is how to deal with nodes that do not cooperate. Depending on their motivation we can categorize these nodes into three groups:

- Malevolent nodes – Nodes that want to compromise the security of the MANET or of other nodes. Their actions are directed on some desired effect, but they are generally not rational because they do not strive for their own benefit maximization.
- Selfish nodes – Nodes that do not forward other's packets, thus increasing their benefit at the expense of all others. They are assumed to always behave rationally, so they cheat only if it gives them an advantage.
- Erroneous nodes – These are nodes with failing hardware or incorrect software. They do not intentionally misbehave but if they impair the working of the net, then they have to be treated just as malevolent or selfish nodes..

III. Dynamic Source Routing

DSR is a kind of source routing based on-demand protocol[1]. DSR routing protocol includes two procedures: route discovery and route maintenance.

A. Route Discovery

When node S is to send message to the destination node D, it first queries if there exists route from S to D in the routing buffer. If so, then source node S sends message according to the route, otherwise route discovery program is launched, meanwhile source node S floods route request packet RREQ,
When intermediate nodes receive the RREQ message, they test RREQ for the repetition of message. If repetition of request message is found, they are abandoned, otherwise attach their address to the route record in the head part of packet, and then send this packet to all the adjacent nodes. When the destination node finally receives RREQ packet, it copies and reverses the route record of the RREQ packet and sends the route reply message RREP to the source nodes, and returns route response message RREP to source node S. Source node buffers the route information locally for future use when receives the RREP packet.

B. Route Maintenance

Once some nodes find the neighboring link that data is to be sent by is disconnected, they immediately send a route error message RERR to source node S. When the source node receives the error packet, it deletes all the routes that use the invalid link from the buffer, and starts a new route discovery process if necessary. The nodes that forward the error packet along the way delete all the route in the broken link from their own routing table.

The route discovery procedure of DSR protocol often discovers many routes from source node to destination node. And route with minimal hop is more possible chosen for data transmission than others, the nodes frequently chosen are more likely to consume more energy, which results in short usage of battery.

IV. Detection and Prevention of Selfish Node

The security problem and the misbehavior problem of MANETs have been studied by many researchers. Different techniques have been proposed to prevent selfish nodes in MANETs. These schemes can be broadly classified into two categories as Credit-Based schemes and Reputation-Based schemes [5].

A. Credit Based Schemes

The basic 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. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services.Credit based schemes can be implemented using two models:

1. The Packet Purse Model (PPM)
2. The Packet Trade Model (PTM)

The Packet Pursue Model (PPM)

In this model, the originator of the packet pays for packet forwarding service. When sending the packet, the originator of the packet loads it with a number of beans sufficient to reach the destination Each forwarding terminal node acquires one or several beans from the packet and thus, increases the stock of its beans. The number of beans depends on the direct path on which the packet is forwarded (long distance requires more beans). If a packet does not have enough beans to be forwarded, then it is discarded. The basic problem with this approach is that it might be difficult to estimate the number of beans that are required to reach a given destination. If the originator underestimates this number, then the packet will be discarded, and the originator loses its investment in this packet. If the originator over-estimates the number, then the packet will arrive, but the originator still loses the remaining

beans in the packet.

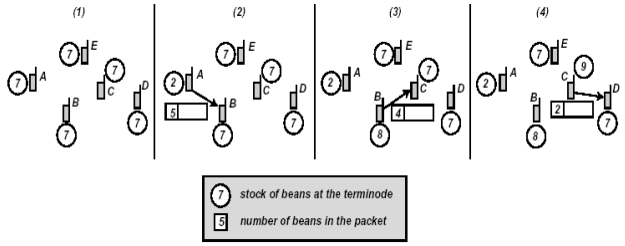

Fig 1 Packet pursue model

The Packet Trade Model (PTM)

In this approach, the packet does not carry beans, but it is traded for beans by intermediate terminal nodes. Each intermediary buys it from the previous one for some beans, and sells it to the next one (or to the destination) for more beans. In this way, each intermediate node that provides a service by forwarding the packet increases its number of beans, and the total cost of forwarding the packet is covered by the destination of the packet. An advantage of this approach is that the originator of the packet does not have to know in advance the number of beans required to deliver a packet. Furthermore, letting the destination pay for the packet forwarding makes this approach applicable in case of multicast packets as well. A disadvantage is that this approach for charging does not directly prevent users from flooding the network.

B. Reputation Based Schemes

In such 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. There are two models for reputation based schemes.

1. Watchdog Model
2. Pathrater

Watchdog Model

The watchdog method detects misbehaving nodes. Suppose there exists a path from node S to node D through intermediate nodes A, B, and C. Node A cannot transmit directly to node C, but it can listen in on node B's traffic. Thus, when A transmits a packet for node B to forward to node C,A can often tell if B transmits the packet. If encryption is not performed separately for each link, which can be expensive, then A can also tell if B has tampered with the payload or the header[6].

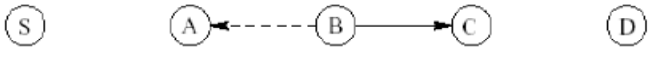

Fig 2 Working of Watchdog

When B forwards a packet from S toward D through C, A can overhear B's transmission and can verify that B has attempted to pass the packet to C. The solid line represents the intended direction of the packet sent by B to C, while the dashed line indicates that A is within transmission range of B and can overhear the packet transfer. Watchdog can be implemented maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer period than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node. DSR with the watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level.

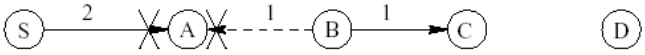

Fig.3 Node A does not hear B forward packet 1 to C, because B's transmission collides at A with packet 2 from the source S.

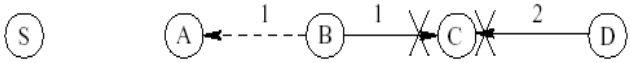

Fig . 4 Node A believes that B has forwarded packet 1 on to C, though C never received the packet due to a collision with packet 2.

Disadvantages of watchdog are that it might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior, and partial dropping. The ambiguous collision problem prevents A from overhearing transmissions from B.

As Figure 3 illustrates, a packet collision can occur at node A while it is listening for B to forward on a packet. A does not know if the collision was caused by B forwarding on a packet as it should or if B never forwarded the packet and the collision was caused by other nodes in A's neighborhood. Because of this uncertainty, A should not immediately accuse B of misbehaving, but should instead continue to watch B over a period of time. If A repeatedly fails to detect B forwarding on packets, then A can assume that B is misbehaving[4].

In the receiver collision problem, node A can only tell whether B forwards the packet to C, but it cannot tell if C receives it as shown in Figure 4. If a collision occurs at C when B first forwards the packet, A only sees B forwarding the packet and assumes that node C has successfully received it. Thus, B could skip retransmitting the packet and leave A none the wiser. B could also purposefully cause the transmitted packet to collide at C by waiting until C is transmitting and then forwarding on the packet. In the first case, a node could be selfish and do not want to waste its power with retransmissions. In the latter case, the only reason B would have for doing such is that it is malicious. B wastes

battery power and CPU time, so it is not selfish. An overloaded node would not engage in this behavior either, since it wastes badly needed CPU time and bandwidth. Thus, this second case should be a rare occurrence[4]. Another problem can occur when nodes falsely report other nodes as misbehaving. A malicious node could attempt to partition the network by claiming that some nodes following it in the path are misbehaving

Pathrater

The pathrater , run by each node in the network, combines knowledge of misbehaving nodes with link reliability data to choose the route which is most likely to be reliable. Each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path[6]. If there are multiple paths to same destination we choose the path with highest metric. Since the pathrater depends on knowing the exact path a packet has traversed, it must be implemented on top of a source routing protocol.

The pathrater assigns ratings to nodes according to the following algorithm[4]. When a node in the network becomes known to the pathrater (through route discovery), the pathrater assigns that node ,a "neutral" rating of 0.5. A node always rates itself with a 1.0. This ensures that when calculating path rates, if all other nodes are neutral nodes (rather than suspected misbehaving nodes), the pathrater picks the shortest length path. The pathrater increments the ratings of nodes on all actively used paths at periodic intervals of 200 ms. An actively used path is one on which the node has sent a packet within the previous rate increment interval. The maximum value a neutral node can attain is 0.8. A node's rating is decremented by 0.05 when we detect a link break during packet forwarding and the node becomes unreachable. The lower bound rating of a "neutral" node is 0.0. The pathrater does not modify the ratings of nodes that are not currently in active use. When the pathrater calculates the path metric, negative path values indicate the existence of one or more suspected misbehaving nodes in the path. If a node is marked as misbehaving due to a temporary malfunction or incorrect accusation it would be preferable if it were not permanently excluded from routing. Therefore nodes that have negative ratings should have their ratings slowly increased or set back to a non-negative value after a long timeout.

V. CONCLUSIONS

In this paper, many different techniques for detection of selfish nodes in MANETs have been discussed. The credit-based scheme is to provide incentives in terms of electronic payments/ beans for nodes to faithfully perform networking functions. 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. In reputation based scheme, network nodes collectively detect and declare the misbehavior of a suspicious node. Such a declaration is then propagated throughout the network. The 2ACK technique is based on a simple 2-hop acknowledgment packet that is sent back by the receiver of the nexthop link.

REFERENCES

[1] David B.; Johnson David A.; Maltz Josh Broch. DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. *Ad Hoc networking 2001*; Vol 5, pp. 139-172.

[2] Natarajan Meghanathan and Levon Paul Judon, " Improvement in Network Lifetime for On-Demand Routing in Mobile Ad hoc Networks Using either On-Demand Recharging or Transmission Power Control or Both", *Computer and Information Science*, Vol. 3, No. 1, Feb. 2010, pp 3-11.

[3] Martin Schutte "Detecting Selfish and Malicious Nodes in Mobile Ad hoc Networks"

[4] Sergio Marti; T.J. Giuli; Kevin Lai; Mary Baker "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks " *Proceedings of Mobicom 2000*, Boston, USA, August 2000

[5] Neeraj Tantubay, Dinesh Ratan Gaitam and Mukesh Kumar Dhariwal "A Review of Power Conservation in Wireless Mobile Ad-hoc Network (MANET) ", International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

[6] Dipali Koshti, Supriya Kamoji "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", International Journal of Soft Computing and Engineering , Volume-1, Issue-4, September 2011

[7] Hemang Kothari , Manish Chaturvedi " Effect of Selfish Behavior on Power Consumption in Mobile Ad Hoc Network" ,Proceedings of the Asia-Pacific Advanced Network 2011

[8] V.Giri Babu,T.Sreenivasulu"Detection of selfish node and replica allocation over MANETs",International Journal of Advance research in Computer Science and Software Engineering, Volume-3,Issue-9,September 2013

[9] Gurjeet Singh "Security Threats and Maintaince in Mobile Adhoc Networks", Internation journal of Electronics and Communication Engineering,Volume-2,Issue -3,2011

[10] Patwardhan A,Parker J, Joshi A, Iorga M, and Karygiannis T,(2005) „Secure routing and intrusion detection in Ad hoc networks," in Proc. 3rd Int. Conf.Pervasive Comput.Commun , pp. 191

[11] Mahmoud, M.E.; Xuemin Shen, "Credit-Based Mechanism Protecting Multi-Hop Wireless Networks from Rational and Irrational Packet Drop," *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, vol., no., pp.1,5, 6-10 Dec. 2010

[12] K. Balakrishnan, J. Deng, and P.K. Varshney. TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks , Proc. IEEE Wireless Comm and Networking Conf. (WCNC"05), Mar. 2005,Volume 4,Pages 2137-2142, IEEE Press 2005,Year of Publication:2005