TECHNIQUES USED FOR DETECTION OF SELFISH NODES IN MOBILE AD HOC NETWORKS

K.P. Shanmuga Priya
(Dept of ECE, KGiSL Institute of Technology, Coimbatore, India, shan.05.priya@gmail.com)

Abstract— *A MANET (Mobile Ad-hoc Network) is a self-configuring system of mobile nodes connected by wireless links. MANETs are self-configuring and decentralized without having a fix infrastructure. In such a network each node acts as an end system as well as a relay node (or router). Most of the routing algorithms designed for MANET such as AODV and DSR are based on the assumption that every node forwards every packet. But in practice some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and also bandwidth for retransmitting the data of other nodes and they reserve them only for themselves. The original AODV and DSR routing algorithms can be modified to detect such selfish nodes. This paper discusses two techniques namely Reputation based technique and Credit based technique used to detect selfish nodes in MANET. This paper concentrate on two algorithms that are based on reputation based technique and one algorithm based on credit based technique. All the three techniques have been compared finally.*

Keywords— MANET; Selfish Nodes in MANET; Misbehaving Nodes in MANET; Cooperative System in MANET

1. INTRODUCTION

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid- to late 1990s. A MANET (Mobile Ad-hoc Network) [1] is a self-configuring system of mobile nodes connected by wireless links. In a MANET, the nodes are free to move randomly, changing the networks topology rapidly and unpredictably. MANETs are decentralized, and therefore all network activities are carried out by nodes themselves. Each node is both an end-system as well as a relay node (router) to forward packets for other nodes. Most of the routing algorithms designed for MANET such as DSR [2], [3] and AODV [4] are based on the assumption that every node forwards every packet. But some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and also bandwidth for retransmitting the data of other nodes and they reserve them only for themselves. This paper discusses two techniques namely reputation based technique and credit based technique to detect selfish nodes in MANET.

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. Credit based schemes 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. The paper discusses two algorithms that are based on reputation based technique and one algorithm based on credit based technique. All three techniques have been compared.

2. RELATED WORK

The techniques for preventing selfishness in MANETs can be categorized as Credit-Based schemes and Reputation-Based schemes [5].

A. Credit Based Schemes

Credit-based schemes 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: The Packet Purse Model (PPM) and the Packet Trade Model (PTM).

1) The Packet Purse Model: The originator of the packet pays for the packet forwarding service. The service charge is distributed among the forwarding nodes. The originator loads it with the number of beans sufficient to reach the destination. Each forwarding node acquires one or several beans from the packet and thus, increases the stock of its beans. If packet does not have enough beans to be forwarded, the packet 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.

2) The Packet Trade Model: The packet does not carry beans but it is traded for beans by intermediate nodes. Each intermediary buys it from previous one for some beans and sells it to the next one for more beans. The total cost of forwarding the packet is covered by destination of the packet. An advantage of this approach is that the originator does not have to know in advance the number of beans required to deliver a packet.

B. 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. There are two models for reputation based schemes. 1. Watchdog Model 2. Path rater

1) Watchdog: With this simple approach a node sends a packet to its neighbour and then overhears the neighbour forwarding it one hop further along the route. Thus a misbehaving node dropping or manipulating packets is immediately identified and routes using this node can be avoided (using a so-called path rater component to choose the best route).

Unfortunately this mechanism is too simple and has two major drawbacks. First: it is error-prone; a packet collision between AB causes a false negative detection (A does not recognize successful retransmission) and a collision between BC causes a false positive detection (A acknowledges the retransmission even though it failed). The model also relies on all clients to have equal sending ranges – this conflicts with modern WiFi-controllers using energy control. Second: When a node recognizes its neighbour as non-participating it does not speed this information, but is only supposed to find a new route around the problem, thus even rewarding the non-participating node (now it does not have to forward other node's data anymore). For the node on its own it is perfectly rational to avoid the selfish node and increase its own throughput – but for the net at large this is a bad choice as it does not punish the selfish node but only burdens the cooperating ones with more work.

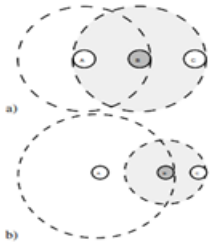

Fig.1 . Watchdog (the shaded area is B's radio range):a) with equal ranges A can overhear B's re-transmission: b) with power control A cannot overhear B's Transmission

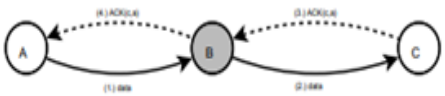

Fig 2. 1. A sends for c; 2.B has to forward the packet as it does not know if it contains ACK request ; 3. Confirms the retrieval with its private key 4. Forwards the ACK back to A.

The Bayesian Watchdog has been developed, a tool that merge the watchdog with Bayesian filters. It is more robust against environmental noise but consume more CPU resources. An adaptation of the watchdog presented above to the Network Simulator 2. It is designed to be use with the AODV protocol of this simulator but can easily adapted to other protocols.

1) Detection speed

Accuracy is a key issue when detecting black holes, but speed is also important. A watchdog that detects 100% of black holes but requires 10 minutes is a useless watchdog. So, it is crucial for accuracy and speed to be well balanced. In that sense, watchdog enhancements will target both speed and accuracy issues. The collaborative Bayesian watchdog performed well in terms of speed. Table IV shows that, on average, 7% of the times our approach detected black holes before the Bayesian watchdog, with the same traffic pattern. The rest of the cases, it detects the malicious nodes at the same time. When a node B enters2 node A's neighbourhood, our approach allows node A to identify node B as a black hole with only a reputations sharing phase with its common neighbour. This means that even if node B does not send or receive any data or routing packet when enters node A's neighbourhood, if it has been previously detected as black hole, node A will quickly mark it as a black hole too.

PERCENTAGE OF DETECTIONS WHERE THE COLLABORATIVE BAYESIAN WATCHDOG DETECTS THE BLACK HOLES BEFORE THE BAYESIAN WATCHDOG DOES IT

Node Speed (m/s.)	Percentage of earlier detections
5	1.04%
10	11.88%
15	9.66%
20	5.72%

2) Path rater

The path rater, run by each node in the network, combines knowledge of misbehaving nodes with link reliability data to pick the route 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. If there are multiple paths to the same destination, the path with the highest metric is chosen.

3. DISCUSSION

This section discusses three different algorithms to detect selfish node in MANET. Two of which use reputation based technique to solve the problem and one uses credit based technique. The proposed 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to moderate their undesirable effect. This paper focuses on the following routing misbehavior.

A selfish node does not perform the packet forwarding function for data packets unrelated to itself. However, it operates normally in the Route Discovery and the Route Maintenance phases of the DSR protocol. Since such misbehaving nodes participate in the Route Discovery phase, they may be included in the routes chosen to forward the data packets from the source. The misbehaving nodes, however, refuse to forward the data packets from the source. This leads to the source being confused. In some networks, a router may be considered well-behaved as long as it sends out the packet toward the next-hop node. This, however, does not guarantee the successful reception of the packet at the next-hop node. Such a behavior by the router, if consistently repeated, is be considered as misbehavior.

A) The 2ACK Scheme

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. Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, this technique focuses on the problem of detecting misbehaving links instead of misbehaving nodes.

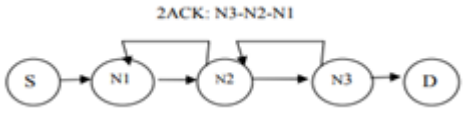

Fig.3. 2ACK Frame

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. Figure 3 illustrates the operation of the 2ACK scheme. Suppose that N1, N2, and N3 are three consecutive nodes (triplet) along a route. The route from a source node, S, to a destination node, D, is generated in the Route Discovery phase of the DSR protocol. When N1 sends a data packet to N2 and N2 forwards it to N3, it is unclear to N1 whether N3 receives the data packet successfully or not. Such an ambiguity exists even when there are no misbehaving nodes. The 2ACK scheme requires an explicit acknowledgment to be sent by N3 to notify N1 of its successful reception of a data packet: When node N3 receives the data packet successfully, it sends out a 2ACK packet over two hops to N1 (i.e., the opposite direction of the routing path as shown), with the ID of the corresponding data packet. The triplet [N1-> N2- > N3] is derived from the route of the original data traffic. Such a triplet is used by N1 to monitor the link N2 -> N3. 2ACK transmission takes place for every set of triplets along the route. Therefore, only the first router from the source will not serve as a 2ACK packet sender. The last router just before the destination and the destination will not serve as a 2ACK receiver. In order to reduce the additional routing overhead, only a fraction of the received data packets are acknowledged.

B) A Reputation-Based Mechanisms to enforce Cooperation in MANET

In [7] the system uses the reputation based approach for detecting misbehaving nodes in MANET. The method detects selfish nodes as well as enforces the selfish nodes to cooperate in MANET. In addition to this, system also encourages cooperating nodes by providing them faster service. This approach to detect selfish nodes has three main modules. Checking system, reputation system and priority processing system.

1) Checking System : In each node, there is a watchdog module that its duty is monitoring the neighbor nodes and observing their behaviors. These observations are the first hand information that is limited to the wireless radio range of a node. However, first, each node will check its first hop neighbors, and then it will save the number of packets which are sent and received by the nodes and next it will send them to the reputation system. This module upgrades the saved information in a specific time period.

2) Reputation System: The reputation system uses the proportion of the number of Packets which are sent by a node to the number of Packets which are received by a node as the cooperation coefficient of a node. This coefficient is the same as Reputation and considered as follow: Cooperation coefficient A is computed as,

A = No. of sent packets/No. of received packets

In each node there is a table which is used to maintain the reputation of the nodes which should check and monitor (First hop neighbors). 'A' is a number between zero and one. The values which are near to zero show that the cooperation of node is low and it is a selfish node but the values which are near to one show the cooperation and as a result the reputation of node is high. In this approach, instead of sending too much messages about the reputation of nodes and also sending the warning messages about the selfish nodes, with adding a new field to the route request message and inserting the cooperation coefficient in it, the number of messages will be reduced, considerably. In this operation, each source node put a primary value as the default cooperation coefficient in this field and then it will send the route request message. The node, which receives this packet, checks the Src-Addr field of packet. If the source node be in the group of nodes which should check by this node, it gets the cooperation coefficient of the node from the reputation table and puts the real coefficient of a node, which is resulted from checking the operations of nodes, in the cooperation coefficient field of packet. It should be considered that only the first hop neighbor of a node has the permission to change and upgrade the cooperation coefficient field of route request packet.

3) Priority Processing System: The priority module determines the priority of each packet depends on the cooperation coefficient field of it. When the node receives multiple packets and the simultaneous forwarding of packets is not possible, the packet of the node whose cooperation coefficient is higher will be forwarded first. Therefore, the cooperator nodes will be encouraged by receiving the services earlier and the selfish nodes will be punished by receiving the services later. Figure 4 illustrates whole process of reputation based mechanism that enforces cooperation in MANET.

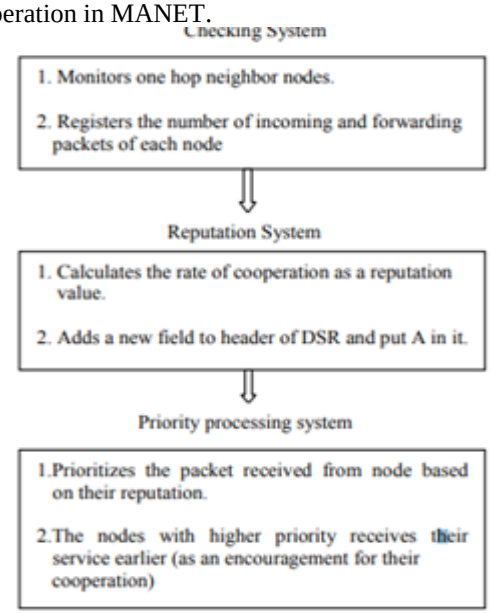

Fig.4. Process of reputation based mechanism to enforce cooperation in MANET

C) An Auction based AODV Protocol for Mobile Ad Hoc

Networks with Selfish Nodes

In [8] Authors have proposed an algorithm which is based on credit system. In-order to deal with selfishness, digital economy is created in the network. In this virtual economy, a source node has to pay some amount of a digital currency to intermediate nodes to have its packet forwarded, whereas the intermediate nodes bid and declare the amount of currency that they would request from the source if they forward the packet. These entire bids node chooses the route with the lowest bid. The source node sends the payment with every packet. Payment is set in a way that every node gets a payment that is greater than the amount that it bid. When nodes bid, they consider their energy level and the amount of currency that they have. Their bid increases when their energy level goes down, and decreases when their currency level goes down. Consequently, an auction based routing mechanism will help to deal with selfish nodes in the network, and also help to increase fairness in distributing the energy consumption in the network.

Maximum value auctioning strategy

(i) The bids for the end-to-end routes are obtained by multiplying the maximum bid for intermediate nodes (maximum of all the bids for all the intermediate nodes on a route) for each route, with the number of intermediate nodes on that route.

(ii) The route with the smallest bid wins the auction.

(iii) The winning route is paid the second lowest bid.

Bidding Formula

To model a realistic relationship among the node's bid, its energy, and its current currency level, authors have impose several properties:

• When a node's energy goes down and its currency stays the same, its bid should go up. This means that when a node has less energy, its willingness to forward packets for others will decrease.

• When a node's currency goes up and its energy goes down, its bid should go down, since its willingness to forward packets for others will not be as high as when it had less currency and high energy.

• When both of a node's currency and energy go down, the decreasing energy will drive the bid up, whereas decreasing currency will drive the bid down. In this case, we prefer to favor on the energy's side than the currency's side. That means that the effect of the change in currency should be less than the effect of the change in energy.

The reason for this choice is that if a node dies, there is not much use for it to have currency. Based on the above requirements, a bidding valuation computation formula is given as:

$$b = a * (\log (C) / Er)$$

Where, b: The bid value of the node, C: Node's current currency amount, Er: The node's energy ratio (Current energy / initial Energy). Here, 'a' is a constant that is chosen as a parameter which influences how high and how fast bids can go up.

1) Modifications to Classic AODV

Nodes must hold in the routing table, three more information fields about a destination:

- The lowest route bid for the destination
- The second lowest bid for the destination
- The nodes own bid for the destination

When a node has a packet to send, it looks at its routing table to see if it has a valid route towards destination. Here, "validity" also requires having information at least on the lowest route bid. If it has valid route info, and if there is a second lowest bid on the routing table, then the node selects the lowest bid route to send its packets, while paying the second lowest bid. If a node does not have a valid route to the destination it sends a route request with a maximum bid value in it. When the route request is sent by a source, the maximum bid value is 0. This value increases as the request makes its way towards the destination. When an intermediate node receives a route request packet, it updates its reverse route and it checks its own routing table for the destination. If it has a "fresh enough" route for the destination, it produces a route reply. In the route reply packet, the node includes its maximum bid. If it does not have a fresh enough route for the destination, then it checks the maximum bid value in the route request packet. If its own bid is greater than the maximum bid value, then it puts its own bid as the maximum bid value in the route request packet and forwards it. Otherwise, it leaves the maximum bid as it is. Note that the node's bid is included in the reverse route towards the source.

4. CONCLUSION

In this paper two techniques are discussed: Reputation based and credit based technique for detection of selfish nodes in MANET. Two algorithms discussed here are based on the reputation based scheme and one is based on credit based scheme. The 2ACK scheme uses the reputation based approach to detect and mitigate the effect of misbehaving nodes in MANET. It serves as an add-on technique for routing scheme to detect routing misbehavior and to moderate undesirable effect. The main idea is to send the two hop acknowledgement packets in opposite direction of the routing path. In order to reduce the additional routing overhead, only a fraction of the received data packets are acknowledged. Thus it detects the selfish nodes, eliminates them and chooses the other path for transmitting the data. In Reputation based approach [7], in addition to punishing the selfish nodes, and encouraging the cooperating nodes, there is second chance for the nodes which dropped a packet unwillingly. In this approach if the node is recognized to be a selfish node for the first time and punished, the cooperation coefficient of it can be increased if it changes its behavior as a cooperator node. The third algorithm "An auction based AODV protocol' uses auctions for an ad hoc network that consists of selfish nodes. It is based on incentivizing cooperation by balancing two different metrics: The residual energy and current currency level of the nodes in the network. The proposed auctioning approach is implemented at the route level, rather than at each intermediate node, thus guaranteeing that a successful bid leads to an end-to-end

transmission route. In future, detecting and correcting the selfish nodes can be implemented. Efficiency and data accessibility can be improved.

REFERENCES

[1] L. Buttyan and J. P. Hubaux, "Stimulating Cooperation in Self Organizing Mobile Ad Hoc Networks", in ACM Journal For Mobile Networks (MONET), Special Issue On Mobile Ad Hoc Network, 2003.
[2] Dave B. Johnson and David A. Maltz, "The dynamic source routing protocol for mobile ad hoc networks", in Internet Draft, Mobile Ad Hoc Network (MANET) Working Group, IETF, Oslo, Norway.
[3] David B. Johnson, David A. Maltz and John Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks" in Ad hoc Networking edited by Charles E. Perkins, Chapter 5, pp. 139-172. (2001)
[4] Ian D. Chakeres and Elizabeth M. Belding-Royer," AODV Routing Protocol Implementation Design" Proceedings of the International Workshop on Wireless Ad Hoc Networking, Tokyo, Japan, March 2004.
[5] V. Srinivasan, P. Nuggehalli, C.F. Chiasserini and R.R Rao," Cooperation in wireless Ad Hoc Network", in IEEE INFOCOM,California,USA,2003.
[6] Zahara Safaei , Mohammad Hossein Anisi an Fatemeh Torgheh, " A Reputation-Based Mechanisms to enforce Cooperation in MANETs", Software, Telecommunications and Computer Networks, 2008(SoftCOM 2008.) 16th International Conference on 25-27 Sept. 2008.
[7] Cenker Demir and Cristina Comaniciu , "An Auction based AODV Protocol for Mobile Ad Hoc Networks with Selfish Nodes", IEEE International Conference