2011 International Conference on Computer and Software Modeling
IPCSIT vol.14 (2011) © (2011) IACSIT Press, Singapore

Detection of Routing Misbehavior in MANETs

S. D. Khatawkar[1], U. L. Kulkarni[2] and K. K. Pandyaji[3+]
[1] ADCET, Ashta, [2] KGCET, Karjat, [3] ADCET, Ashta.

Abstract: This paper highlights routing misbehavior in MANETs (Mobile Ad Hoc Networks). In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. However, due to the open structure and scarcely available battery-based energy, node misbehaviors may exist. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets.
In this paper, different schemes are to be discussed that serves as an add-on technique to detect routing misbehavior and to mitigate their adverse effect.

Keywords: Mobile Ad Hoc Networks (MANETs), routing misbehaviour, node misbehaviour, network security, Dynamic Source Routing (DSR), Trusted Credit Clearance Service (TCCS).

1. Introduction

MANETs are two types: closed and open. In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be most important in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes, and their behaviour is termed selfish or misbehaviour. One of the major sources of energy consumption in mobile nodes of MANETs is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

2. Related Schemes

The security problem and the misbehaviour problem of wireless networks including MANETs have been studied by many researchers. Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be broadly classified into two categories: Credit-based schemes and Reputation-based schemes.

2.1 The Packet Purse Model (PPM)

In this model, the originator of charge is distributed among the forwarding terminal nodes in the following way: When sending the packet, the originator 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 connection 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. Packet forwarding in the Packet Purse Model is illustrated in Figure 1. The basic

[+] shriharikhatawkar@gmail.com

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 packet3.

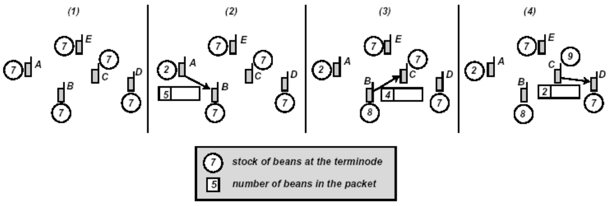
(1)
(2)
(3)
(4)
A
B
C
D
E
7 stock of beans at the terminode
5 number of beans in the packet

Figure 1: The Packet Purse Model

2.2 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 intermediary that provided 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.

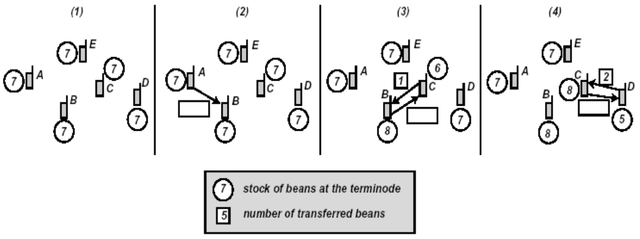
(1)
(2)
(3)
(4)
A
B
C
D
E
7 stock of beans at the terminode
5 number of transferred beans

Figure 2: The Packet Trade Model

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. 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.

2.3 Watchdog

The watchdog method detects misbehaving nodes. Figure 2 illustrates how the watchdog works. Suppose there exists a path from node S to D through intermediate nodes A, B, and C. Node A cannot transmit all the way to node C, but it can listen in on node B's traffic. Thus, when A transmits a packet for B to forward to 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.

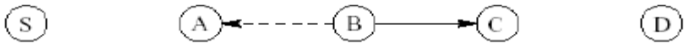

Fig. 3

Figure 3: 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. We implement the watchdog by maintaining a offer 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 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 misbehaviour at the forwarding level and not just the link level.

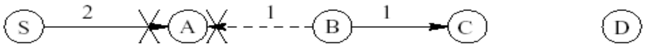

Fig 4: Node A does not hear B forward packet 1 to C, because B's transmission collides at A with packet 2 from the source S.

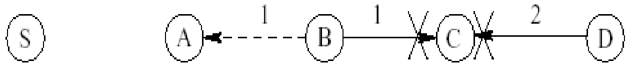

Figure 5: Node A believes that B has forwarded packet 1 on to C, though C never received the packet due to a collision with packet 2.

Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehaviour, 5) collusion, and 6) partial dropping. The ambiguous collision problem prevents A from overhearing transmissions from B. As Figure 3 illustrates, a packet collision can occur at 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 neighbourhood. 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. In the receiver collision problem, node A can only tell whether B sends the packet to C, but it cannot tell if C receives it (Figure 4). If a collision occurs at C when B first forwards the packet, A only sees B forwarding the packet and assumes that C successfully receives 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 not want to waste power with retransmissions. In the latter case, the only reason B would have for taking the actions that it does because 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. 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.

2.4 Pathrater

The pathrater, 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. We choose this metric because it gives a comparison of the overall reliability of different paths and allows pathrater to emulate the shortest length path algorithm when no reliability information has been collected, as explained below. If there are multiple paths to the same destination, we choose the path with the highest metric.

2.5 Sessions-based Misbehavior Detection Protocol (SMDP)

This solution consists of two related stages: the monitoring stage, in which nodes monitor their direct neighbours when forwarding packets, and the decision stage, where nodes decide about the behaviour of each monitored node basing on the result of the previous stage.

A. Monitoring Stage: In Sessions-based Misbehaviour Detection Protocol (SMDP), each node in the route session monitors all of its direct neighbours (i.e. neighbours within a one hop communication), and checks whether they correctly forward packets. We define a session as the continuous traffic sent from the source node to the final destination node. The routing protocol has to be aware of the beginning and the end of session. This has been done through cross layer

B. Decision Stage: The new monitoring method allows the neighbouring nodes to judge whether each monitored node in the session has forwarded packets correctly or not.

2.6 Fair incentive protocol (FIP)

To realize the credit-based incentive strategy, the following assumptions are raised.

1) Each mobile node should have a unique nonzero ID, a pair of certificated public and private keys, and can support cryptographic operations.

2) Each mobile node should have a credit account to store its credits, which are used for paying the other nodes packet forwarding assistance. In general, a mobile node can earn credits in the following two ways: i) purchase credits with real money; and ii) receive credits by forwarding packets for the other peer nodes. Similar to the credit cards in the real life, a mobile node is allowed to request services first and perform the credit clearance operation with the Trusted Credit Clearance Service (TCCS) later on.

3) The TCCS is trusted and has a pair of public and private keys, which fairly performs credit clearance operations for the mobile nodes.

4) The communication between the mobile nodes is bidirectional, i.e., two nodes within the wireless transmission range may directly communicate with each other based on the popular wireless 802.11 protocol. However, due to the nature of mobility, the wireless channel may be unreliable

5) A mobile node can report to the TCCS for credit clearance, through a fast and secure channel.

A. Fairness Objectives

In a civilian selfish MANET with an incentive strategy, some mobile nodes could still be selfish and cause unfair events while forwarding packets. This happens in the following two situations, which will be considered in this study: i) after the intermediate nodes forward packets for the source node to the destination node, the source node collude with the destination node to deny paying the credits to the intermediate nodes. ii) The intermediate nodes which have obtained the credits from the source nodes are still reluctant to forward packets for the source nodes. Both of the situations result n unfairness and may yield fatal impact on the system cooperation. In this study, an atomicity principle is defined: “The intermediate nodes can receive credits if and only if the destination node receives the packets.” which will serve as the basis in the design of our incentive strategy. According to the atomicity principle, we subtly depict four states as shown in Fig. 6 which demonstrates the relation between the fairness and incentive strategy in the MANET.

STATE 0 has no incentive strategy and fairness issue, where all mobile nodes are selfish and no-cooperate. Thus, the whole network is in degradation.

STATE “1” is fair and the whole network lies in its optimum cooperative status. All the mobile nodes are normal-behaved due to the incentive strategy, and the atomicity principle follows.

STATE “2” is unfair. Although the incentive strategy is injected, the source or destination nodes are still selfish as in case i). Due to this unfairness, the whole network cannot reach its optimum cooperative status.

STATE “3” is also unfair. The unfair status is due to the selfishness of the intermediate nodes as described in case ii). The whole ad hoc network is in degradation.

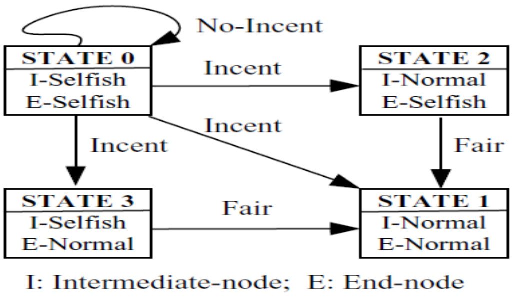

Fig.6. Fair incentive state transition model for ad hoc networks

Based on the above state definition, the fairness objectives in this work is to provide efficient fairness strategy to push unfair STATE 2 and STATE 3 to the optimum cooperative STATE 1 status. To the best of our knowledge, no previous work has worked out a good solution for this purpose.

2.7 THE ‘2ACK’ SCHEME

The watchdog detection mechanism has a very low overhead. Unfortunately, the watchdog technique suffers from several problems such as ambiguous collisions; receive 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. 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: It will not be forwarded further. The result is that this link will be tagged. Our approach discussed here significantly simplifies the detection mechanism.

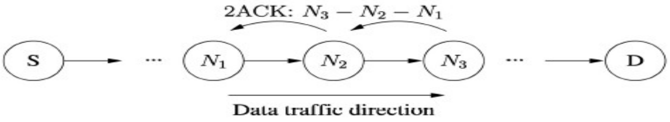

Fig.7. 2ack scheme

3. Conclusions

In this paper, many different techniques for detection of selfish nodes have been discussed which effect the performance degradation in MANETs.

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. A new low cost approach for monitoring node misbehaviour in MANET is the SMDP. It reduces the communication overhead by using only one hop communication (no flooding), and sending control packets only at the end of sessions, instead of doing so for each packet. FIP provides incentive to mobile nodes to cooperate in selfish MANETs. It does not require any tamper-resistant device but achieve the fairness between the source /destination nodes and intermediate nodes. The 2ACK technique is based on a simple 2-hop acknowledgment packet that is sent back by the receiver of the next-hop link. Compared with other approaches, the 2ACK scheme overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers.

4. References

[1] K. J. Liu, J. Deng, P. Varshnet and K. Balakrishnan. An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs” *IEEE TRANSACTIONS ON MOBILE COMPUTING*, VOL. 6, NO. 5, MAY 2007.

[2] T. Fahad, D. Djenouri, R. Askwith1, M. MerabtiJ and C. Maxwell. A new low cost Sessions-based Misbehaviour Detection Protocol (SMDP) for MANET.2007.

[3] R. X. Lu, X. D. Lin, H. J. Zhu, C. X. Zhang, P.-H. Ho and X. M. (Sherman) ShenI. A Novel Fair Incentive Protocol for Mobile Ad Hoc Networks, in the WCNC 2008 proceedings.

[4] A. Mohammed, M. Ould-Khaoua and L. M. Mackenzie. Improvement to Efficient Counter-based Broadcast Scheme through RandomAssessment Delay Adaptation for MANETs. Second UKSIM European Symposium on Computer Modeling and Simulation.

[5] K. Vijaya. SECURE 2ACK ROUTING PROTOCOL IN MOBILE AD HOCNETWORKS

[6] K. Balakrishnan, J. Deng and P.K. Varshney. TWOACK: Preventing Selfishness in MobileAd Hoc Networks. 2005.