Selfish Nodes Detection using Random 2ack in MANET's

G.Muruga Boopathi, N.Insozhan, S.Vinod

Abstract- A Mobile Ad Hoc Network (MANET) is a temporary infrastructure less network, formed by a set of mobile hosts that dynamically establish their own network without relying on any central administration. Mobile ad hoc networking works properly only if the participating nodes cooperate in routing and forwarding. However, performing network functions consumes energy and other resources. To save its energy a node may behave selfishly and uses the forwarding service of other nodes without correctly forwarding packets for them. These nodes must be identified and excluded from the cooperative part of the network, as they only consume resources and don't contribute to the infrastructure. In MANET's routing misbehavior can severely degrade the performance at the routing layer. Specifically, nodes may participate in the route discovery and maintenance process but refuse to forward data packets. Some solutions have been detected to mitigate such selfish nodes. But almost all these solutions rely on the watchdog technique in their monitoring components, which suffers from many problems. Here we approach a new method where past problems are being addressed and will assess its performance. Misbehavior detection systems aim at removing the MANET vulnerability. We propose a system to detect misbehaving nodes in mobile ad hoc networks.

Keywords: Mobile Ad Hoc Networks, Routing misbehavior, Selfishness, Network security.

I. INTRODUCTION

Ad-hoc wireless networks are peer-to peer networks where each computer with a wireless interface can communicate directly with participating nodes. These nodes can self- organize without central management and special infrastructure. The network is established using (limited range) radio communication where each node acts as both data terminal and data transfer equipment. Moreover, nodes can move freely resulting in changes to the network topology and updated routing in order to forward the packets. The topology change depends on different factors such as mobility model, node speed etc.

Manuscript received on February, 2013.

G.Murugaboopathi received the Undergraduate Degree in Computer Science and Engineering from Madurai Kamaraj University, in 2000, the Post Graduate degree in Digital Communication and Network from Madurai Kamaraj University, in 2002 and Ph.D in Computer Science and Engineering at Bharath University, Chennai.

N.Insozhan received the Undergraduate Degree in Information and technology from Annamalai University, in 2005, the Post Graduate degree in Computer Science and Engineering from Annamalai university. He has more than 05 publications in National, International Conference. He has more than 4 years of teaching experience.

S.Vinod received the Undergraduate Degree in Computer Science and Engineering from Anna university, in 2007, the Post Graduate degree in software Engineering from Anna university. He has more than 05 publications in National, International Conference. He has more than 3 years of teaching experience.

Due to the infrastructure less nature of MANETs packets sent between distant nodes are expected to be relayed by intermediate ones, which act as routers and provide the forwarding service

The forwarding service is closely related to the routing. It consists in correctly relaying the received packets from node to node until reaching their final destination, following routes selected and maintained by the routing protocol. The nature of MANET makes cooperation among nodes essential for the system to be operational. In some MANET's applications where all nodes belong to a single authority (in the application layer point of view) and have a common goal, e.g.-soldiers in a military unit during a battlefield or rescuers in a rescue team during a rescue operation, nodes are cooperative by nature. In MANETs critical functions like routing and forwarding performed by less trusted and less secured nodes. Indeed, nodes try to preserve their resources, and particularly their batteries. 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. Intentionally uncooperative behavior (misbehavior) may result in a total communication breakdown. A node may behave selfishly by agreeing to forward the packets and then failing to do so due to Overloaded, Selfish, Malicious or Broken. Behavior node models Collaborative model: A node that behaves properly executing both packet forwarding and routing functions. Selfish model: A node that misbehaves to save its battery life. This node could disable packet forwarding and/or routing functions. Malicious model: A node that aims at damaging other nodes by causing network out age by partitioning while saving battery life is not a priority.

II. CREDIT-BASED SCHEMES

Credit based schemes work on a give and take basis. These schemes work on the principle that you get credit for every packet you forward, and pay some of the credit to send a message yourself. Buttyan and Hubaux used the concept of nuggets (also called beans) as payments for packet forwarding. They proposed two models: the Packet Purse Model and the Packet Trade Model. In the Packet Purse Model, nuggets are loaded into the packet before it is sent. The sender puts a certain number of nuggets on the data packet to be sent. Each intermediate node earns nuggets in return for forwarding the packet. If the packet exhausts its nuggets before reaching its destination, then it is dropped. In the Packet Trade Model, each intermediate node "buys" the packet from the previous node for some nuggets and "sells" it to the next node for more nuggets. Thus, each intermediate node earns some nuggets for providing the forwarding service and the overall cost of sending the packet is borne by the destination. When the nodes get a connection to a Credit Clearance Service, they report those credits, and based on the decision taken by the CCS the nodes need to pay or they may be rewarded with real money.

Since this system uses an external party for the payment, it may not be useful for all scenarios.

III. THE RANDOM 2ACK SCHEME

We use 2ACK to detect routing Misbehavior. The 2ACK scheme is a network layer technique to detect selfishness and to mitigate their effects. It can be implemented as an add-on to existing routing protocols for MANETs, such as DSR. 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. The following example illustrates the operation of the 2ACK scheme. Suppose that A, B, and C 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 'A' sends a data packet to B and B forwards it to C, it is unclear to 'A' whether C receives the data packet successfully or not. Such an ambiguity exists even when there are no misbehaving nodes. The problem becomes much more severe in open MANETs with potential misbehaving nodes.

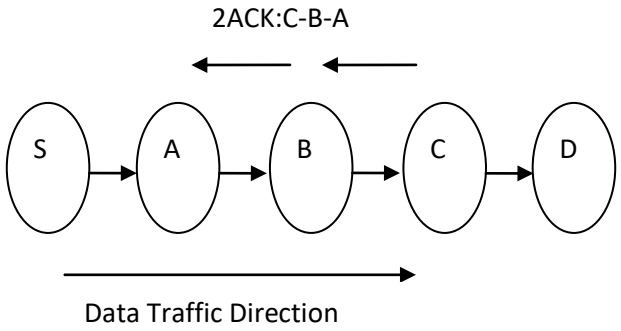

Fig 1: The 2ACK Scheme

The 2ACK scheme requires an explicit acknowledgment to be sent by C to notify 'A' of its successful reception of a data packet: When node C receives the data packet successfully, it sends out a 2ACK packet over two hops to 'A' (i.e., the opposite direction of the routing path as illustrated in above fig 1), with the ID of the corresponding data packet. The triplet [A _ B_C] is derived from the route of the original data traffic. Such a triplet is used by 'A' to monitor the link B_C. For convenience of presentation, we term 'A' in the triplet [A_B_C] the 2ACK packet receiver or the observing node and C the 2ACK packet sender.

Such a 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 2ACK receivers.

B Next Hop Receiver	C Second Hop Receiver	C_{pkts} Packets Transmitted	C_{mis} 2 ACK Packets Missed	LIST List of data packet IDs

Fig2. Data structure maintained by the observing node.

To detect misbehavior, the sender maintains a list of IDs of data packets that have been sent out but have not been acknowledged. For example, after 'A' sends a data packet on a particular path, say, [A _B_C] , it adds the data ID to LIST (refer to Fig. 2,which illustrates the data structure maintained by the Observing node), i.e., on its list corresponding to B_C. counter of forwarded data packets, Cpkts, is incremented simultaneously. At node 'A', each ID will stay on the list for seconds, the timeout for 2ACK reception. If a 2ACK packet corresponding to this ID arrives before the timer expires, the ID will be removed from the list. Otherwise, the ID will be removed at the end of its timeout interval and a counter called Cmis will be incremented. When C receives a data packet, it determines whether it needs to send a 2ACK packet to 'A'. In order to reduce the additional routing overhead caused by the 2ACK scheme, only a fraction of the data packets will be acknowledged via 2ACK packets. Such a fraction is termed the acknowledgment ratio, Rack. By varying Rack, we can dynamically tune the overhead of 2ACK packet transmissions. Node 'A' observes the behavior of link B_C for a period of time termed Tobs. At the end of the observation period, 'A' calculates the ratio of missing 2ACK packets as Cmis/Cpkts and compares it with a threshold Rmis. If the ratio is greater than Rmis, link B_C is declared misbehaving and 'A' sends out an RERR (or the misbehavior report) packet. Since only a fraction of the received data packets are acknowledged, Rmis should satisfy Rmis > 1 - Rack in order to eliminate false alarms caused by such a partial acknowledgment technique. Each node receiving or overhearing such an RERR marks the link B_C as misbehaving and adds it to the blacklist of such is behaving links that it maintains. When a node starts its own data traffic later, it will avoid using such misbehaving links as a part of its route. As Compared with the overhearing techniques, such as watchdog, the 2ACK scheme solves the problems of ambiguous collisions, receiver collisions, and limited transmission power: The obvious problem of our first solution i.e. the 2ACK scheme is the important overhead it engenders, even if the nodes well behave. It requires a two-hop ACK for each data packet, which is costly. In order to reduce the additional routing overhead, this proposes a new technique termed random 2ACK. In this only a fraction of data packets will be acknowledged via 2ACK packets.

IV. CONCLUSION

In mobile ad hoc networks, nodes act both as terminals and information relays, and they participate in a common routing protocol, such as Dynamic Source Routing (DSR). The nature of ad hoc networks is dynamically changing. However, due to the open structure and scarcely available battery-based energy, node misbehavior may exist. The Mobile ad hoc network is vulnerable to many attacks, due to faulty or malicious nodes. Packet dropping is the most common attack. However, the lack of a common goal in MANETs without a centralized human authority will make them difficult to maintain: each user will attempt to retrieve the most of the network while expecting to pay as less as possible. In human communities, this kind of behavior is called selfishness. While prohibiting selfishness shows to be impossible over a decentralized network, applying punishments to those that present this behavior may be beneficial. As we have seen, the watchdog technique, used by almost all the solutions currently proposed to detect nodes that misbehave on packets forwarding in MANETs, fails when employing the power control.

We propose a new method termed random 2ACK, to detect and mitigate the effect of such routing misbehavior. The random 2ACK technique is based on a simple 2-hop acknowledgment packet that is sent back by the receiver of the next-hop link.

ACKNOWLEDGEMENT

The Authors sincerely thank the chairman of VelTech group of institution Col.Prof. Dr.Vel Sri.R.Rangarajan, Chairperson and Managing Trustee, Director for their encouragement to prepare this review. They further extends sincere thanks to Principal and Head of the department of Information Technology of Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College for their constant support at every stage to complete this review.

REFERENCES

1. 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.
2. Kejun Liu, Jing Deng, Pramod K.Varshney, Kashyap Balakrishnan"An Acknowledgement-Based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing vol.6,No.5,May 2007.
3. S.Marti,T.Giuli,K.Lai and M.Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks",Aug 2000.
4. Djamel Djenouri, Nadjib adache,"New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks".

AUTHORS PROFILE

G. Murugaboopathi, received the Undergraduate Degree in Computer Science and Engineering from Madurai Kamaraj University, in 2000, the Post Graduate degree in Digital Communication and Network from Madurai Kamaraj University, in 2002 and Ph.D in Computer Science and Engineering at Bharath University, Chennai. He has more than 20 publications in National, International Conference and International Journal proceedings. He has more than 10 years of teaching experience. His areas of interest include Wireless Sensor Networks, Mobile Communication, Mobile Computing, Mobile Adhoc Networks, Computer Networks, Network Security, High Speed Networks, Network and Data Security, Cryptography and Network security, DBMS and etc., He is currently working as an Head R & D and Associate Professor in the Department of Information Technology at Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College Chennai India.

N. Insozhan, received the Undergraduate Degree in Information and technology from Annamalai University, in 2005, the Post Graduate degree in Computer Science and Engineering from Annamalai university. He has more than 05 publications in National, International Conference. He has more than 4 years of teaching experience. His areas of interest include Wireless Sensor Networks, Mobile Communication, Mobile Computing, Mobile Adhoc Networks, Computer Networks, Network Security, High Speed Networks, Network and Data Security, Cryptography and Network security, DBMS and etc., He is currently working as Assistant Professor in the Department of Computerscience and Engineering at Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College Chennai, India.

S. Vinod, received the Undergraduate Degree in Computer Science and Engineering from Anna university, in 2007, the Post Graduate degree in software Engineering from Anna university. He has more than 05 publications in National, International Conference. He has more than 3 years of teaching experience. His areas of interest include Wireless Sensor Networks, Mobile Communication, Mobile Computing, Mobile Adhoc Networks, Computer Networks, Network Security, High Speed Networks, Network and Data Security, Software Engineering, DBMS and etc., He is currently working as Assistant Professor in the Department of Computer science and Engineering at Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College Chennai, India.