Volume : 2 | Issue : 5 | May 2013 • ISSN No 2277 - 8179

Research Paper

Selfish Nodes Detection in MANETs: Acknowledgement Based Approacht

Engineering

KEYWORDS : MANET, Selfish Nodes in MANET, Routing- Protocols, Acknowledgement Based Selfish-node detection

Swati L. Kariya — Department of Computer Science and Engineering, Gujarat Technological University

Bakul B. Panchal — Department of Computer Science and Engineering, Gujarat Technological University

ABSTRACT

Wireless networking is a popular technology that allows users to access information and services electronically, regardless of their geographic position. It has opened the doors for new emerging applications in the domain of networking. One emerging and promising areas is the domain of Mobile Ad Hoc Networks (MANETs).

I. Introduction

In this era of Wireless Communications and wireless devices like Laptops, PDAs, Mobile Ad Hoc Network becomes a very popular networking paradigm for communication. A mobile ad hoc network is a network that consists of mobile nodes that communicate wirelessly and does not have an infrastructure or pre-fixed topology [1]. Nodes in mobile ad hoc network communicate through either single-hop or multi-hop modes. Therefore, in this environment, each node acts as a router as well as a host. But communication is possible only if nodes participate and route other node's packets.

So, Routing protocols [8] of MANET based on the assumption that all the nodes behave cooperatively, but on the other hand every node has to consider its limited resources like CPU Power, Battery, bandwidth and energy. Hence some nodes behave selfishly and do not forward other's packets, thus maximizing their benefit at the expense of all others. They are called as Selfish nodes.

The next section lists various behaviours of selfish-nodes in MANET.

II. Selfish nodes behaviour in manet

Here the list of attacks [2] is given which Selfish nodes can do on MANET:

- Do not participate in routing either by Do not relay route re quests or replies
- Modifies routing data/topology by adding additional hops or by modifying route reply or by changing the original ID of Sender or receiver.
- Dropping Data packets either full or partial to save its own energy in forwarding.
- By setting TTL or hop limit
- Provoke route error

Every attack given here affects to the packet delivery ratio, throughput, power consumption and many more parameters of the network. Thus it is very requisite to detect the selfish nodes for proper functioning of MANET. So this paper discusses various Acknowledgement based strategies available for the detection of these selfish nodes from the ad-hoc network and a new proficient Acknowledgement based strategy is proposed which is going to be discussed in next section.

II. Related work

There are several schemes that use end-to-end acknowledgments (ACKs) to detect routing misbehaviour and selfish-nodes in wireless network. 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 and these schemes has focus on detection of selfish nodes based on this sending of Acknowledgements by destination.

To prevent selfishness in MANET, Balakrishnan [3] proposed a TWOACK scheme which can be implemented as an add-on to any source routing protocol. In this scheme TWOACK packet is sent on successful reception of every data packet, which is assigned a fixed route of two hops in the direction opposite to that of data packets. Basic drawback of this scheme includes it detects misbehaving links instead of particular misbehaving node thus sometimes even well behaving nodes became part of misbehaving link and therefore cannot be further used the network. Thus a lot of well behaved node may be avoided by network which results in losing of well behaved routes.

To improve the TWOACK, Vijaya [4] has proposed another acknowledgement based scheme in which it detects misbehaving link, eliminate it and choose the other path for transmitting the data. The main idea is to send 2ACK packet which is assigned a fixed route of two hops back in the opposite direction of the data traffic route and to reduce the additional routing overhead, a fraction of the data packets will be acknowledged via a 2ACK packet. This scheme also consists of multicasting method by which sender can broadcast information of misbehaving nodes so that other nodes can avoid path containing misbehaving nodes and take another path for the data transmission. Thus routing overhead is minimized but it also suffers from misbehaving nodes detection.

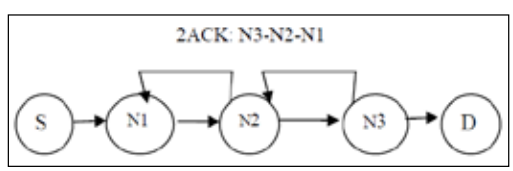
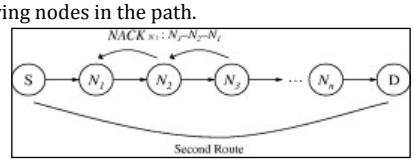


Fig.1 2ACK Scheme

The NACK scheme is proposed by Usha and Radha [5], an extension to the TWOACK scheme, is trying to isolate misbehaving nodes in a MANETs. Here in this scheme, each intermediate node also has to send an ACK packet after it receives data packet from the immediate sender, if the acknowledgement fails to arrive within the stipulated time immediate sender retries for K times then it declares the current node as misbehaving. Hence here each intermediate node has to send ACK to its immediate sender after receiving data packet and the destination node sends a NACK after receiving each packet from the sender, which must be forwarded by in the same path in which the initial transmission took place.

On receipt of the Nack packet, the source node compares the two paths that are in the Nack packet. If variation is found, then the node in the source to destination path, from where the path varies in the destination to source path is isolated and that particular node is marked as a potential misbehaving node by the source node otherwise source node concludes no potential misbehaving nodes in the path.



Volume : 2 | Issue : 5 | May 2013 • ISSN No 2277 - 8179

Fig. 2 NACK Scheme
Possible drawback includes a lot of routing overhead because of Ack and Nack packets, which slows the performance and throughput of the network and due to mobility, probability of Nack packet reaching to source becomes smaller with the large number of intermediate nodes between source and destination.

IV. Proposed approach

In this section, we elaborate more details of our solution to address the routing misbehaviour and selfish node detection. The whole scheme is divided into three activities. First activity will identify malicious activity if any, in the network.

For the same, in the proposed SACK-Selfish node detection scheme, instead of sending back an acknowledge packets all the time when a data packet is received, a node wait until a certain amount of data packets of the same source node arrive, then it sends back one SACK packet acknowledge for multiple data packets that have been received. Thus it reduces a lot the overhead of acknowledgement routing. If the source node does not get SACK packet by intermediate nodes after some prefixed time T, then it gives indication about some malicious action in the network.

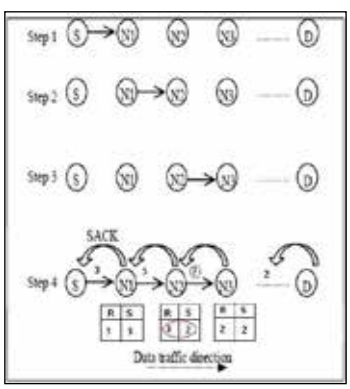


Fig.3 Proposed SACK-Selfish node

Detection Scheme
Second activity is about identification of particular misbehaving node in network. For that the monitoring algorithm called PACKET CONSERVATION MONITORING ALGORITHM (PCMA) [6] have been used in proposed approach, because most of the other mechanisms give the suspicious node i.e. selfish node with some degree of trust, but here this algorithm completely avoids any trust for the selfish node by relying only on information from the neighbouring nodes of the suspicious node, and not all of the neighbouring nodes, but only neighbouring nodes that sent/received a direct information from or to the suspicious node and by doing this, we will save power which is important in MANET.

As illustrated in Fig. 3, by using the approach of PCMA algorithm, we will maintain the data as a table of sent and received packets for each node of the network. Through that we can identify easily, by comparing the values of R and S for individual node as shown in figure, which node is working as a packet dropper for the network and not sending the packets further in the network by behaving selfishly.

The third activity is about isolation of the misbehaving node and for isolation, after caught by PCMA if the node is misbehaving, source node will broadcast about the misbehaviour and selfishness of the node that it can be avoided in future routing process and depend upon protocol it can choose different path which does not have any selfish nodes.

V. Conclusion

This paper presents a frame work in detecting misbehaving selfish nodes that are dropping packets and isolating such nodes from routing process in MANETs. Mainly our scheme has advantage of less routing overhead because it uses the concept of selective acknowledgement and then too it can detect the selfish node very effectively with less efforts, by just maintaining table of sent and received packets. Hence throughput, packet delivery ratio and thus the performance of overall network can be significantly improved by detecting these selfish nodes efficiently and this scheme can be combined on top of any source routing protocol such as AODV. Currently we are working on its simulation in ns-2 simulator [7] to show the results and effectiveness of our solution on AODV routing protocol [8]. Similar approaches can also be integrated to these source routing algorithms to address other attacks like black hole and gray hole attacks in MANETs.

Acknowledgment
We would like to thank reference authors and also like to thank Professors, family and friends for supporting us.

REFERENCE

[1] S. Alampalayam, A. Kumar, and S. Srinivasan, "Mobile ad hoc network security-a taxonomy," Advanced Communication Technology, ICACT 2005., pp. 839-844, 2005. | [2] Abdelaziz Babakhouya, Yacine Challal, and Abdelmadjid Bouabdallah, "A Simulation Analysis of Routing Misbehaviour in Mobile Ad Hoc Networks," in Proc. of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies, September 2008, pp. 592-597. | [3] K. Balakrishnan, J. Deng, and P. K. Varshney. TWOACK: preventing selfishness in mobile ad hoc networks. In Proc. Of IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, March 2005. IEEE. | [4] Mrs. K. Vijaya, "Secure 2ACK Routing Protocol in Mobile Ad hoc Networks", TENCON.2008 | [5] Usha.Sakthivel and Radha.S "Routing layer Node Misbehavior Detection in Mobile Ad hoc Networks using N-ack Scheme" (ICTEEP'2012) July, 2012 | [6] Tarag Fahad & Robert Askwith, "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks", ISBN: 1-9025-6013-9, 2006 | [7] The Vint Project, "The ns-2 network simulator," http://www.isi.edu/nanam/ns | [8] Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010 ISSN: 2010-0248 |