A Survey on Selfish Node Detection using Several Techniques in Manet

K.Sridevi, S.Kannan

Abstract— The term MANET (Mobile Ad-hoc Network) refers to a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self-organizing and adaptive network that can be formed and deformed on-the-fly without the need of any centralized administration. In practice some of the nodes in MANET act as selfish node that is such kind of nodes reserve their resource and energy for its own use but they do not cooperate with other nodes in the network. This paper discusses several techniques to detect selfish nodes in MANET.

Keywords— MANET, Selfish nodes in MANET.

I. INTRODUCTION

MANET is a self-creating, self-organizing and self-administering wireless network. Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. It is a self-configuring network of mobile nodes connected by wire-less links the union of which forms an arbitrary topology. The nodes are free to move randomly and organize them-selves arbitrarily thus, the network's wireless topology may change rapidly and unpredictably. Each node in a MANET acts as a router, and communicates with each other. A large variety of MANET applications have been developed [27]. For example, a MANET can be used in special situations, where installing infrastructure may be difficult, or even infeasible, such as a battlefield or a disaster area. Such networks are aimed to provide communication capabilities to areas where limited or no communication infrastructures exist.

The characteristics of selfish nodes as follows:

- Do not participate in routing process: A selfish node drops routing messages or it may modify the Route Request and Reply packets by changing TTL value to smallest possible value.
- Do not reply or send hello messages: A selfish node may not respond to hello messages, hence other nodes may not be able to detect its presence when they need it.
- Intentionally delay the RREQ packet: A selfish node may delay the RREQ packet up to the maximum upper limit time. It will certainly avoid itself from routing paths.
- Dropping of data packet: A selfish nodes may participate in routing messages but may not relay data packets.

This paper discusses several non-cooperative techniques namely credit based technique and cooperative techniques namely reputation based technique to detect selfish node in mobile ad-hoc networks.

II. RELATED WORK

1. CREDIT BASED METHOD

Dipali Koshti, Supriya Kamoji says the techniques for preventing selfishness in MANET by credit based. The concept of credit based system is to provide incentive for nodes that forward data to the neighbouring nodes i.e., nodes that perform completely in the network. Nodes get paid for their services. Credit based schemes can be implemented using two models: The Packet Purse Model (PPM) and the Packet Trade Model (PTM).

In the Packet Purse Model, the author says, the originator of the packet pays for the packet forwarding service. 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.

In the Packet Trade Model, the author says they buy for some beans and forward it for some more beans. 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.

1.1 Secure Incentive Protocol

This approach assumes that each mobile node (MN) has a tamper-proof security module such as SIM cards in GSM networks, which deals with security related functions and each intermediate node (IN) puts non-forged stamps on the forwarded packets as a proof of forwarding. Secure Incentive Protocol, (SIP) uses "credits" as the incentives to stimulate packet forwarding. The charging and rewarding on a node is done by decreasing or increasing the CC in that node. Advantages of this method are SIP is routing independent in the sense that it could coexist with any on demand unicast routing protocol such as DSR and AODV. SIP is session based rather than packet based. Security module is tamper proof and hence unauthorized access is not allowed. But the problem with this approach is, it needs every node to possess the hardware module and SIP is implemented in the hardware module. Hardware module will not be available in the already existing mobile nodes.

1.2 Stimulating Cooperation in Self Organizing Manets

L.Buttayan et al's approach uses a tamper resistant hardware module called "security module". This security module maintains a nuglet counter. The nuglet counter is protected from illegitimate manipulations by the tamper resistance of the security module.

Revised Manuscript Received on December 22, 2012.

K.Sridevi, Computer Science Department, SNS College of Technology Coimbatore

S.Kannan, Computer Science Department, SNS College of Technology Coimbatore

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

This approach ensures that the misbehavior is not beneficial and hence it should occur rarely only. But the availability of hardware module is not guaranteed.

1.3 Sprite

In Sprite, proposed by Zhong et al. nodes keep receipts of the received/forwarded messages. When they have a fast connection to a Credit Clearance Service (CCS), they report all these receipts. The CCS then decides the charge and credit for the reporting nodes. The limitation of Sprite is that CCS is assumed to be reachable through the use of Internet.

1.4 N-ACK Scheme

The Nack scheme extends the 2 Ack scheme in trying to isolate misbehaving nodes in a MANETs. The Nack scheme requires an end to end Ack packet to be sent between the source and the destination. The destination on receipt of the data packets sent by the source, responds with a Nack packet.

Each node maintains a list of data packets sent and another list of data packets forwarded.

On receipt of the Nack packet, the source node compares

the two paths that are in the Nack packet. If there is no variation in the paths, then the source node concludes that there are no potential misbehaving nodes in the path. In case the two paths vary, the node in the source to destination path, from where the path varies in the destination to source path is isolated. This node is marked as a potential misbehaving node by the source node. For each potential misbehaving node, a threshold is maintained. If the number of times a node

is adjudged as a potential misbehaving node exceeds the threshold, then the node is flagged as misbehaving and information is sent to all the neighboring nodes advising them about the misbehaving node in the actual message packet, delivered to the destination.

1.5 Collective Network Arbitration Protocol (CNAP)

The author [8] says, as a prerequisite each node is expected to maintain a set of information about each of its neighboring nodes. Each node maintains a counter (Car) for each of the node in its neighbourhood list. This counter is initiated to zero and can have a maximum value equal to a threshold (UL) which is predefined.

1.6 Contribution time-based Selfish Node Detection

The author [2] says, each monitoring node operates in promiscuous mode and would monitor both data and control packets that are sent around within its receiving range. Each monitoring node will keep a record for each of its neighboring node. In the INETMANET [16] framework, there is already a specific table to store the information about the neighboring nodes. The author adds extra fields to the table such as follows:

last_action is the time the neighboring node is last seen contributing or providing services to the network. last_request on the other hand is the time recorded the neighboring node is last seen utilizing or requesting for services from the network. These two fields would be updated for every action observed due to the promiscuous mode monitoring. Finally, status is the current behavior of the neighboring node detected by the monitoring node. The initial status for any node is set to zero as for unknown and could later be changed to suspicious or behaved.

Here each monitoring node will only consider its own personal discovery and will not share this observation to other nodes. This eliminates most trust management complexity and avoids any false accusation and false praise attacks.

III. REPUTATION-BASED METHODS

The author [1] says that, 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.

2.1 Watch Dog and Path Rater

The author describes two mechanisms to improve the throughput of the network. One mechanism is the watchdog, which identifies the misbehaving node by monitoring the nearby nodes whether they forward the packets of other nodes in the network. The other mechanism is the path rater that defines the best route by avoiding those misbehaving nodes. But this approach does not isolate the misbehaving nodes; they still utilize the network services, i.e. the nodes are not punished for misbehaving.

2.2 The 2ACK Scheme

The author Dipali Koshti, Supriya Kamoji proposes the 2ACK scheme in reputation based techniques for selfish node detection in mobile ad-hoc network. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. 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.

2.3 A Reputation-Based Mechanisms to enforce Cooperation in MANET

The author Dipali Koshti, Supriya Kamoji proposes this scheme in reputation based techniques for selfish node detection in mobile ad-hoc network. This mechanism detects selfish nodes using three modules- Checking System, Reputation System and Priority processing System.

Monitors one hop neighbor nodes and registers the number of incoming and forwarding packets of each node. Then it upgrades the saved information in a specific time period.

Calculates the rate of cooperation as a reputation value and adds a new field to header of DSR and put cooperation coefficient in it. 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. Prioritizes the packet received from node based on their reputation. The nodes with higher priority receives their service earlier (as an encouragement for their cooperation). Therefore, the cooperator nodes will be encouraged by receiving the services earlier and the selfish nodes will be punished by receiving the services later.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

2.5 CORE

Michiardi and Molva [4] proposed a Collaborative Reputation (CORE) mechanism where the reputation values are obtained by regarding nodes as requesters and providers, and comparing the expected result to the actually obtained result of a request. In CORE the reputation value ranges from positive (+) through null (0) to negative (-). The advantage of this method is that having a positive to negative range allows good behavior to be rewarded and bad behavior to be punished. This method gives more importance to the past behavior. But the assumption that past behavior to be indicative of the future behavior may make the nodes to build up credit and then start behaving selfishly.

2.6 CONFIDANT

CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad-hoc Networks), [] has four interdependent modules (a) monitor, (b) reputation system, (c) path manager, (d) trust manager. Monitor collects evidence by monitoring the transmission of a neighbor after forwarding a packet to the neighbor. It then reports to the reputation system only if the collected evidence represents a malicious behavior. Reputation system changes the rating for a node if the evidence collected for a node's malicious behavior exceeds the pre-defined threshold value. Then, path manager makes a decision to delete the malicious node from the path. Trust manager assists in making trust decisions for the following, whether to: provide and accept routing information, accept a node as a part of route, and take part in a route originated by some other node.

IV. CONCLUSIONS

The work was initiated with an intention of carrying out exhaustive study of the selfish node detection in Mobile Ad hoc Network to improve their performance. This deals with the two classifications of methods to detect selfish nodes in MANET. According to the empirical study we cannot say this technique is best fit for all the situations to give accurate result.

ACKNOWLEDGMENT

The authors would like to express their thanks to Dr.S.Karthik M.E., Ph.D., DEAN cum Professor and Head Department of Computer Science and Engineering, SNS College of Technology for support and environment provided for research.

REFERENCES

1. Dipali Koshti and Supriya Kamoji, "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", IJSCE, vol. 1, issue – 4, September 2011.
2. Khairul Azmi Abu Bakar, "Contribution Time-Based Selfish Node Detection Scheme, 2001.
3. Prasanna Padmanabhan, Le Gruenwald, Anita Vallur and Mohammed Atiquzzaman, "A survey of data replication techniques for mobile ad hoc network databases", the VLDB Journal, 2008.
4. Pietro Michiardi and Refik Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia, 2002.
5. S.Marti, T.Giuli, K.Lai and M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks," in Proc. ACM MOBICOM, pp. 25
6. Sangheethaa Sukumaran , Venkatesh.J and Arunkorah, "A Survey of Methods to mitigate Selfishness in Mobile Ad hoc Networks", International JICT, vol. 1, no. 2, June 2011.
7. Shailender Gupta, Nagpal.C.K. and Charu Singla, " Impact of Selfish Node Concentration in MANETs", International Jpurnal of Wireless & Mobile Networks (IJWMN), vol. 3, no.2,April 2011.
8. Takahiro Hara, " Effective Replica Allocation in Ad hoc Networks for Improving Data Accessibility, " IEEE INFOCOM, 2001.
9. Takahiro Hara, Norishige Murakami and Shojiro Nishio, "Replica Allocation for Correlated Data Items in Ad Hoc Sensor Networks", SIGMOD Record, vol. 33, no.1, March 2004.
10. Usha.S, "Multi Hop Acknowledgement Scheme based Selfish Node Detection in Mobile Ad hoc Networks", International Journal of Computer and Electrical Engineering, Vol. 3, No. 4, August 2011.
11. Yang Zhang, "Balancing the Trade-Offs between Query Delay and Data Availability in MANETs", IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 4, April 2012.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication