A Survey Of Selfish Node Identification Techniques In Mobile Ad Hoc Network

Smita Rukhande*
Fr. CRIT, Vashi, Mumbai University

Prasanna Shete
K.J.Somaiya COE,Vidyavihar,Mumbai University

Abstract— ***Mobile Ad hoc Network (MANET) is a collection of mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administer. Because of limited communication range among mobile nodes in ad-hoc network, several network hopes may be needed to deliver a packet from one node to another node in the wireless network. In such a network every node is responsible for forwarding packets to its neighbouring nodes. Due to resource constraints like CPU power, battery and bandwidth some nodes may not participate in forwarding the packets for saving its resources. The presence of selfish behaviour among nodes may lead to network partitioning and makes a major negative impact in the network operation. To avoid such circumstances selfish node deduction is very important. Already many selfish node detection mechanisms have been developed and still exist. And this survey is to evaluate some of the selfish node detection mechanisms and to analyse its merits and demerits. This paper compares different methods based on node's behavioural analysis for reducing the effect of selfish nodes in mobile ad hoc networks.***

Keywords— ***MANET, Selfish Nodes, battery, AODV, DSR***

I. INTRODUCTION

A MANET is a network consists of a group of mobile devices (nodes) communicating through a wireless medium without the need of any fixed infrastructure such as an access point or base station [1]. A node may be able to communicate with other nodes far away with the cooperation of intermediate nodes, forwarding the packets to the destination. Routing protocol such as Dynamic Source Routing [DSR] [2] and AODV [3] have been designed to handle such environment. However, since there is no centralized administration, the performance of a MANET greatly depends on the cooperation of all nodes in the network. Each node operates as both host and router to forward packets for other nodes. Most of the routing algorithms designed for MANET such as DSR and AODV 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 [4] The characteristics of selfish nodes [5] as follows:

- Do not participate in routing process: A selfish node is not forwarding the routing messages or it modifies 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 forward data packets.

Several selfish node detection techniques explored to minimize the network performance degradation, loss of sent packets, network partitioning. This survey mainly focuses on the features, the advantages and the disadvantages of each and every technique for identification of selfish nodes in MANETs. This paper discusses several credit based technique and reputation based technique to detect selfish node in mobile ad-hoc networks. The remainder of this paper is organized as follows. Section II discusses the various issues concerning selfish node in MANETs. Based on the issues, Section 3 review and classifies the existing identification of selfish node techniques for MANET. Finally, Section III concludes the paper and identifies future research directions.

II. ISSUES CONCERNING SELFISH NODE IN MANET

Identification of selfish node technique for MANET must deal with the following issues arising from constraints imposed by their specific environments and applications:

- Network partitioning: Due to presence of selfish node, network partitioning occurs more often in MANET. Network partitioning is a severe problem in MANET when the server that contains the required data is isolated in a separate partition, thus reducing data accessibility to a large extent.
- Throughput: Percentage of packets received by the destination to the number of packets sent by the source is affected by available of selfish nodes in MANET.
- Hop count: A hop is the segment of the route between the source and destination nodes. If number of Selfish nodes increases in MANET, Number of intermediate hops from source to destination increased. It could be decreased the performance of the Network.

- Packet dropping Ratio: Number of packets dropped by the routers due to nodes act as a selfish node for saving its resources.
- Packet Delivery Ratio: It is the fraction of the number of data packets delivered to the destination node from the source node. It is affected by selfish node in MANET.
- End-to-End delay: End-to-end delay is the time consumed by a data packet to be transferred across the MANET from a source node to the destination node. It is increased by selfish nodes in MANET.

These issues could potentially lead to network partitioning and corresponding performance degradation. To minimize such situations in MANETs, many studies have explored in identification of selfish node techniques.

III. IDENTIFICATION OF SELFISH NODES TECHNIQUES

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

A. *Credit Based Techniques*

The basic idea of credit based technique is to 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) [6]. In the Packet Purse Model 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 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) *Stimulating Cooperation in Self Organizing Manets:* Stimulating Cooperation in Self Organizing Manets [7] approach assumes that each mobile node 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 [2]. Secure Incentive Protocol, (SIP) uses “credits” as the incentives to stimulate packet forwarding. For this purpose, each smartcard has a credit counter (CC) which is pre-charged with a certain amount of credits before shipped out[2][3]. The charging and rewarding on a node is done by decreasing or increasing the CC in that node and the CC will retain its value even when mobile node is power off. When mobile node is power-on again, it could still reuse the credits in the CC even in another SIP-enabled ad hoc network. To guarantee the security of SIP, each smartcard contains a private number and a public number (keys). The nodes have no knowledge about the keys stored in the smartcard and could not change CC in an unauthorized way either. SIP is session based and mainly consists of three phases. During the first Session initialization phase, a session initiator (SI) negotiates session keys and other information with a session responder (SR) and INs between them. And each IN puts a non-forged stamp on each data packet forwarded and SI/SR collect those stamps for later rewarding use in the next Data forwarding phase [2]. The final phase is Rewarding phase, in which each IN is awarded a certain number of credits based on the number of forwarded packets. Advantages of this method are 1. SIP is routing- independent in the sense that it could coexist with any on- demand unicast routing protocol such as DSR and AODV. 2. SIP is session based rather than packet based. 3. 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.

2) *Sprite:* Sprite [8] system comprises consists of the Credit Clearance Service (CCS) [6] and a collection of mobile nodes. CCS determines the charge and credit to each node involved in transmission of message. The nodes are equipped with network interfaces that allow them to send and receive messages through a wireless overlay network. To identify each node, sprite assumes that each node has a certificate issued by a scalable certificate authority and the sender knows the full path from the sender to the destination, using a secure ad hoc routing protocol based on DSR. When a node sends its own messages, the node will lose credit to the network because other nodes incur a cost to forward the messages. On the other hand, when a node forwards others messages, it should gain credit and therefore be able to send its messages later. The receiving node also keeps a receipt of message and later forwards them to CCS at fast connection. Thus the sender is charged for the message. Any node engaged in forwarding process is compensated by charges whether or not the transmission is successful. A transfer is considered successful if the next hop neighbour reports a valid receipt to the CCS. There are two ways for a node to get more credit. First, a node can pay its debit or buy more credit using real

money, at a variable rate to the virtual money, based on the current performance of the system. However, the preferred and dominant way to get more credit is by forwarding others messages. Sprite suffers from two main issues. Formerly, since different nodes in the path submit their receipts at different times, it may become difficult for the CCS to determine the actual payment to each node. Also, if routing is based on DSR, some nodes not belonging to DSR path may collude with nodes in the path to forge the receipt and thereby spoof CCS.

B. Reputation Based Techniques

In a reputation based technique, each node is responsible for monitoring the transmission of a packet to neighbour node, or obtaining the status of other nodes from a centralized node on the network. If a node successfully contributes in the transmission of data by forwarding data packets, the reputation of the node is increased, or if the node discards the packet by dropping it, the reputation is decreased. After the nodes reputation drops below a threshold set by the developer, the node is either punished or ignored.

1) *Watchdog and Pathrater:* Marti [9] proposed a scheme for misbehaviour detection which involves two techniques namely Watchdog and Pathrater. In watchdog technique each node has a mechanism which overhears the medium to check whether the next-hop node faithfully forwards the packet or not. Each node maintains buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If it overhears forwarding, removes the packet from the buffer and determined that node as a normal node. If a packet has stayed in the table for longer than a certain period, the module increments a failure count for the node responsible for forwarding on the packet. If the count exceeds a certain threshold value, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node. The Strength of this mechanism is to detect selfish node accurately and to maintain the throughput of the system at an adequate level even with a more number of misbehaving nodes and it can identify selfish node in link layer and network layer. This scheme has several disadvantages. It can’t detect the selfish nodes in case of limited transmission power, ambiguous collision, receiver collision, minor dropping. It is only suitable for source routing protocols such as DSR instead of any general routing protocols. This technique does not penalize the selfish nodes that not cooperate. The watchdog can work only when links are bidirectional. In practical, many unidirectional links may exist in MANETs due to the topology control. Each mobile node requires certain amount of memory space to store packets until proper forwarding by its neighbour is confirmed. These stored packets are used for a comparison with packets forwarded by its neighbouring mobile nodes to check and ensure if the neighbour transmits correct data. As a result, it consumes high volume of storage. Pathrater technique is used for selecting reliable path from source to destination. In this mechanism, each node in the network maintains a rating for all other mobile nodes. It computes “path metric” by averaging the rating of the nodes on the paths and the metric gives a comparison of the overall reliability of different paths. The path with highest metric will be chosen as the reliable path. If any node gets very low rating, it should be considered as a selfish node and thus excludes them from routing. It concentrates to select the reliable path but not deals with recovering the selfish node in MANET. The advantage of pathrater is the throughput increases with the increase in node mobility. The main drawbacks of this approach is that it does not punish selfish nodes and if the mobility of nodes increases overhead also increases.

2) *CONFIDANT Protocol:* CONFIDANT stands for Cooperation of Nodes Fairness in Dynamic Ad-hoc Network [10]. The objective of this system is detecting and isolating misbehaving nodes. In this system, Reputation and trust value is calculated based on the observation and experience about behaviour of other nodes. The system consists of the Monitor, the Trust Manager, the Reputation System and the Path Manager. The monitor does “neighbour watch”, where nodes notifies any malicious act in its neighbourhood. The trust manager deals with incoming and outgoing warning messages. Warning messages are sent by the trust manager of a node to warn others of malicious nodes. Reputation system manages a table which populates itself with rating corresponding to each node. Ratings can be changed when malicious activity seemingly exceeds a predefined threshold. Path Manager is responsible for re-ranking of path according to reputation of constituent nodes. The advantages of this system are no data forwarding service (punishment) is provided for low reputation nodes i.e. misbehaving nodes and it avoids possible bad routes. The drawbacks are inconsistent problem occurs due to each node has different evaluations for same node to detect the selfish node also eavesdropping is not addressed and nodes in a black list are ignored.

3) *CORE:* Michiardi and Molva [11] proposed CORE (Collaborative Reputation Mechanism) to detect and isolate selfish nodes. CORE stimulates node cooperation by a collaborative monitoring technique and a reputation mechanism. Each node computes a reputation value for every neighbour that differentiates between subjective reputation (observation), indirect reputation (positive reports by others) and functional reputation (take-specific behaviour). Two basic components for the CORE mechanism are reputation table and watchdog mechanism [8]. The watchdog mechanism is used to detect misbehaviour nodes. The reputation table is a data structure stored in

each node. Each row of the table consists of four entries: the unique identifier of the entity, a collection of recent subjective observations made on that entity's behaviour, a list of the recent indirect reputation values provided by other entities and the value of the reputation evaluated for a predefined function. The CORE scheme involves two types of protocol entities, a requestor and one or more providers that are within the wireless transmission range of the requestor. If a provider refuses to cooperate (the request is not satisfied), then the CORE scheme will react by decreasing the reputation of the provider. Route tables are updated in two different situations: during the request phase of the protocol and during the reply phase corresponding to the result of the execution. In the first case only the subjective reputation value is updated while in the second case, only the indirect reputation value is updated. The advantages of CORE mechanism is to prevent the DOS attacks and it is impossible for a node to maliciously decrease another node's reputation because there is no negative rating spread between nodes. The limitations of CORE suffers from spoofing attack and it cannot prevent colluding nodes from distribute negative reputation.

4) *Observation-based Cooperation Enforcement in Ad hoc Networks:* Bansal et al [12] proposed a protocol called Observation-based Cooperation Enforcement in Ad hoc Networks (OCEAN) which is an extension of the DSR protocol. OCEAN also uses the monitoring and reputation mechanism [10]. OCEAN classified routing misbehaviour into two classes: misleading and selfish. If a node participates in the route discovery but does not forward a packet, its class is misleading as it misleads other nodes to route packets through it. But if a node does not even take part in the route discovery, it is considered to be selfish. In order to detect the misleading routing behaviours, a node buffers the packet checksum after forwarding a packet to a neighbour, then it can monitor if the neighbour attempts to forward the packet within a given time. As a result of monitoring, either a negative or positive event is produced to update the neighbour rating. If the rating is lower than the faulty threshold, that neighbour node is added to a faulty list. The advantages of OCEAN are it will distinguish the selfish and misleading nodes and it maintains overall network throughput with existence of selfish nodes at network layer. It fails to punish the misbehaving nodes severely.

5) *A reputation-based mechanisms to enforce cooperation in Manet:* Tiranuch Anantvalee and Jie [13] proposed a method that 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 method has three main modules to detect selfish nodes checking system, reputation system and priority processing 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. 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 co-operator nodes will be encouraged by receiving the services earlier and the selfish nodes will be punished by receiving the services later. 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.
'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.

IV. Conclusion

This paper discussed several approaches for dealing with selfish nodes. Selfish nodes are a real problem for ad hoc networks since they affect the network throughput. Many approaches are available in the literature. But no approach provides a solid solution to the selfish nodes problem. The Credit based approach provides incentives to the well behaving nodes and just by passes the selfish nodes in selecting a route to the destination. But selfish node still enjoys services without cooperating with others. The detection and isolation mechanism isolates the selfish nodes so that they don't receive any services from the network. Thus penalizing the selfish nodes. But if many nodes become selfish network communication itself will become impossible. Thus we cannot eliminate all the selfish nodes from the network. A new method to reduce the effect of selfishness and stimulating the nodes to cooperate in the network services should be developed.

References

[1] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan. 1999.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] D. B. Johnson and D. A. Maltz, Yih-Chun Hu, "Dynamic Source Routing in Ad-Hoc wireless Networks", IETF Internet Draft, draft-ietf-manet-dsr-09.txt, April 15, 2003.

[3] C. E. Perkins and E. M. Royer, “Ad Hoc On Demand Distance Vector (AODV) Routing”, Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999.

[4] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang, “Security in mobile ad hoc networks: Challenges and Solutions,” IEEE Wireless Communications, vol. 11, pp. 38–47, 2004.

[5] Shin Yokoyama†, Yoshikazu Nakane, Osamu Takahashi, Eiichi Miyamoto, Nippon information Technology Consulting Co., Ltd. Future University-Hakodate “Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods”. Proceedings of the 7th International Conference on Mobile Data Management (MDM'06) 2006 IEEE.

[6] Dipali Koshti, Supriya Kamoji “Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks”, (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4, September 2011.

[7] L. Buttyan and J.P. Hubaux, “Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks,” ACM/KUler Mobile Networks and Applications, Vol. 8 No. 5 2003.

[8] S. Zhong, J. Chen and Y. R. Yang, “Sprite: A Simple Cheat-Proof, Credit Based System for Mobile Ad hoc Networks”, Proc. INFOCOM, Mar-Apr 2003.

[9] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker “Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks”, ACM 2000.

[10] Sonja Buchegger, Jean-Yves Le Boudec, “Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-Hoc Networks)” ACM June 2002.

[11] 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), 2002.

[12] S. Bansal and M. Baker, “Observation-Based Cooperation Enforcement in Ad hoc Networks," Research Report .NI/0307012, Stanford University, 2003.

[13] Tiranuch Anantvalee and Jie, “Reputation-Based System for Encouraging the Cooperation of Nodes in Mobile Ad Hoc Networks”, 2007 IEEE.