Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Comparative Study of Selfish Node Detection Methods in Manet

Swapnil S. Shinde*, Dr. B. D. Phulpagar
P.E.S. Modern College of Engineering,
Savitribai Phule Pune University
Maharashtra, India

Abstract—Mobile ad hoc networks (MANETs) are infrastructure less and intercommunicate using single-hop and multi-hop paths. Nodes in MANET can act as hosts and routers. Nodes involve themselves in a process of packet forwarding and so the packets are relayed in a cooperative way to the destination point. Topology change is occurring frequently. Due to mobility of nodes routing paths are created and deleted. Every node is provided with limited amount of computation power and battery power. So each node trying to save own resources or trying to consume others resources by showing selfishness thus forms DOS attack by not participating in packet forwarding process which results in network disruption. In this paper we will discuss detection methods along with well-known schemes. Finally all these solution schemes are compared

Keywords— Mobile Ad hoc Network (MANET), Misbehaving node, Selfish Node

I. INTRODUCTION

In the past few years, a rapid expansion and research in mobile computing field is observed due to the availability of large numbers of inexpensive wireless devices. But current devices, applications and protocols are focused on WLAN - wireless local area networks and neglecting the great potential offered by mobile ad hoc networking. A MANET - mobile ad hoc network is an autonomous collection of mobile devices such as smart phones, laptops, sensors, etc. that communicate with each other over wireless links without a fixed infrastructure. To provide the necessary network functionality, nodes cooperate in a distributed manner. MANET, operating as a stand-alone network or can be collaborated to internet or cellular networks, provides the way for variety of new applications. Some of the applications include: personal network, emergency and rescue operations, conference setting, campus settings, car networks, etc. MANET is transient in nature i.e. created on the fly as per requirement where mobility of nodes is not controlled in any way so it's very difficult to assign designated central authority for controlling purpose. Due to the constant change in topology and communication. Links of MANET raises the main problem to find path from source to the destination so that messages may be delivered in time followed by task of performing the secure communication between nodes for a long time period in a hostile environment. MANET can use either proactive type of protocol (DSDV, OLSR) or reactive type of protocol (AODV, DSR) for routing [1]. The nature of MANET poses a range of challenges to the security design such as: an open decentralized peer-to-peer architecture, a shared wireless medium and a highly dynamic topology. The main problem for MANET security resides: it can be reached very easily by users, but also by malicious attackers. If a malicious attacker reaches the network, the attacker can easily exploit or possibly even disable MANET. As MANET is not centrally administered every node has to work and behave in a cooperative way. So the overall performance of MANET is highly depending on nodes and their cooperation towards packet forwarding task. Many different types of attacks have been identified. This paper describes the Denial of service attack (DOS) by a selfish node which is the most common form of attack which affects the network performance. The nodes in ad hoc network have limited battery power and bandwidth, and each node needs the cooperation of other nodes to route its packets forwarded. The selfish nodes are not infected or malicious in nature but are hesitant to spend their resources such as battery power, CPU time, and memory for others [2]. This behavior could cause disturbance in network as nodes are not participating in packet forwarding activity. 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 detection methods concerning selfish node in MANETs. Section III reviews some of the detection schemes for identification of selfish node in MANET. In the same section summarized representation of techniques used to identify selfish nodes is given. Section IV presents the comparison of all schemes and methods and Section V concludes the paper.

II. DETECTION SCHEMES

Several approaches have been proposed for detection of selfish node in MANET. In this section we briefly summarize these approaches. Following are the four main categories of selfish node detection

1. Reputation based Scheme
2. Credit based Scheme

3. Acknowledgement based Scheme
4. Game Theoretic Scheme

1. Reputation Based Schemes:
This scheme works in a collaborative manner. Reputation simply means to opinion about a thing. Here nodes communicate with each other in order to give feedback about particular nodes cooperative behaviour. Every node gives feedback in terms of a reputation value. In this way every node collects high reputation value to build trust and confidence about good behaviour and cooperation in network. Low reputation value is considered to be indication of selfish behaviour while high reputation value indicated cooperative behaviour of nodes. The reputation value of a selfish node is clear indication to the other nodes about its cooperation in the network. The network will detect the selfish nodes then the message about this will get propagated to the whole network and the selfish node will be eliminated from the network [7].

2. Credit Based Schemes:
In this scheme [4] [5], incentive is given to cooperating nodes for the transmission function in network. Main idea here is "serve & earn". This incentive based scheme uses the concept of virtual credit or currency type of payment schemes. The incentives are given for packet forwarding in order to motivate the non-cooperative node to participate. This scheme needs a setup of virtual payment system. It uses two models as follows-
[A] Packet Purse Model:
In this model, the sender of the packet has to pay other intermediate nodes for the packet forwarding service. The sender loads a packet with some number of beans which are sufficient enough to reach the destination. These beans are distributed among the forwarding nodes. Each intermediate node acquires some beans from the packet as a charge of packet forwarding service. In this way each node increases the stock of its beans. The packet is discarded if packet does not have enough beans to forward. The main problem with this model is that the difficulty in estimating the number of beans that are required to reach a given destination node.
[B] Packet Trade Model:
This method overcomes the problem persist in previous method about the estimating total no. of beans in the beginning. In this method the packet does not carry beans instead it will get sold to next node for some beans through trading. Each intermediate node buys the packet from previous node for some beans and sells it to the next node for more beans using trading. The total cost of forwarding the packet will be paid by destination node of the packet.

3. Acknowledgement Based Schemes:
The acknowledgement based schemes ensures the forwarding of a packet by a node using an acknowledgement. In this scheme a node sends an ack packet to source once it is being forwarded. If a source node does not get this ack packet this means misbehaviour of node is observed [6].

4. Game Theoretic scheme:
In game theoretic scheme [13], Nash equilibrium is followed in which two kinds of games are played by the nodes namely Cooperative game & Non-cooperative game. In Cooperative game, a node does communication with each other and behaves in a mutual way. On the other hand, in Non-cooperative game, a node behaves independently. Each node keeps the track of ratio of services provided to services used. Finally system compares node's performance against other node based on a played repeated game. This scheme is lot more easy to implement but it needs a fair criteria to make comparison among nodes otherwise it may lead to false identification of a node as misbehaving node [14].

III. DETECTION TECHNIQUES

As the field of MANETs is increasing day by day, efforts are made to focus on the subject of securing such networks. Most challenging and vital issue is that MANETs must have secure way for transmission and communication. Many researchers and groups have proposed ways to secure the MANET from selfish node attack out of which some are presented below.

1. 2ACK Scheme
K. Balakrishnan et. al. [06] have proposed a scheme called 2ACK scheme which is considered to be a network layer scheme to detect the selfish nodes. This scheme uses an acknowledgement packet called 2ACK packet for detection. In this scheme the next hop node in the route will send back a 2 hop acknowledgment packet i.e. 2ACK. This acknowledgment packet is used to give indication that the data packet has been received successfully. In this process the first router node from the sender will not serve as the sender of 2ACK.

2. Watchdog
Marti et. al. [7] have proposed the watchdog mechanism which is implemented on every node. It monitors nearby nodes in order to identify the misbehaving nodes. When a node forwards a packet to the watchdog, it checks whether the next node in the path will forward this packet or not. If watchdog observes that if the node does not forwarding the packet then it is considered as selfish node. The watchdog will avoid such selfish nodes from the routing path and selects alternative path.

3. Path rater

Marti et. al. [7] have proposed this mechanism where a path metric is calculated for each routing path. This is achieved by setting up a mechanism called as path rater with every node. Each node runs this mechanism and gives rating after every successful transmission of packet. For every path to the particular destination the path metric value is calculated and the path with highest metric will be chosen as the most reliable path.

4. CONFIDANT

Buchegger et. al. [8] have proposed a technique which is somewhat similar to watchdog and path rater and it is known as CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad Hoc Networks). The CONFIDANT protocol contains four important components i.e. Monitoring System, Reputation System, Trust Manager and Path Manager. These components performs function like neighboring node watching, rating of node, rating of path & sending and receiving of alarm messages respectively. This method monitors the behavior of neighbor nodes thus detect the misbehavior node and they will pass this information to Reputation system. This system then modifies the rating of nodes. Once this rating reaches some tolerable range at this time path manager is called to take action. It controls the route cache. Finally ALARM message is sent by trust manager to warn other nodes about misbehaving node.

5. CORE

Michiardi et. al. [9] have proposed CORE (Collaborative Reputation Mechanism) system to improve the coordination among nodes. It uses two basic components which are - 1) Reputation table and 2) Watchdog mechanism. It imposes the cooperation among the nodes by using reputation report mechanism. Each node performs some computation to calculate the reputation value for all neighbor nodes. The reputation report contains values ranges from positive to negative. This mechanism allows to pass only positive reputation reports.

6. OCEAN

Bansal et. al. [10] have proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks). It also runs on monitoring and reputation mechanism. The OCEAN mechanism is basically having following five components 1) Neighbor Watch 2) Route Ranker 3) Rank-Based Routing 4) Malicious Traffic Rejection and 5) Second Chance Mechanism. Each node has rating about other nodes. An update in this rating is made after monitoring certain events. There are two types of events generated i.e. a negative or positive event which are produced based on packet forwarding action. The nodes having rating below some threshold value are getting added to the faulty list. These nodes may become operational after certain time period by assigning a neutral rating to them. Sometimes due to less energy level or weak wireless links or network restart the nodes are not able to rely the packets at this point of time Second chance mechanism helps.

7. SORI

Q. He et.al. [11] have proposed secure and Objective Reputation-based Incentive (SORI) scheme. This method encourages the packet forwarding. It consists of three components and they are (1) Neighbor monitor, (2) Reputation propagation and (3) Punishment. Reputation rate of a node is calculated on the basis of packet forwarding ratio of nodes. This packet forwarding behavior is monitored by neighbor monitor. By using reputation propagation, this information is shared with other nodes. All nodes maintain local evaluation record which represents the confidence metric. The more the packet transmitted to a node for forwarding, the higher is the confidence about trustworthiness of that node. A non-cooperative node is punished by all its neighboring nodes. Punishment will use the information of local evaluation record of a node and the threshold to make decision about the packet dropping.

8. Sprite

Zhong et. al. [12] have proposed a scheme called Sprite. It uses a Credit Clearance Service (CCS). It is used to define the credit and charge of each node. To calculate the charges and credits it uses Game theory methods. Each node will get a receipt of message that it has received or forwarded. Each node keeps the receipt of the message and it will forward the receipt to the CCS. The credit of a node is totally depending on the forwarding behavior of a node. The forwarding is considered as successful only if the next node on the path reports a valid receipt to the CCS. If the node forwards the message then credit will be raised otherwise credit decreases.

Table 1: Comparison between Detection Schemes

Scheme Name	Advantages	Disadvantages
Reputation Based Schemes	Misbehaviour of a node is communicated to all hence it is avoided from route.	Selfish nodes are just bypassed and not punished.
Credit Based Schemes	Central system deals with false positive problem of nodes.	Need of extra protection for the virtual currency hardware.
Acknowledgment Based Schemes	Increased Packet Delivery Ratio.	Message Overhead leads to network congestion
Game Theoretic Schemes	Provides tools to study situations of conflict and cooperation and concerned with finding the best actions for individual decision makers in such situations	It requires additional information per session which leads to overhead.

IV. COMPARATIVE ANALYSIS

The following section will present a comparison between these detection schemes and techniques. Table 1 summarizes the comparison among the schemes while Table 2 shows the comparison between various techniques.

Table 2: Comparison between Detection Techniques

Technique	Advantages	Disadvantages	Protocol Used
Watchdog	• Detect misbehaviour at the forwarding level and link level • Increase in throughput with the increase in node mobility	• No detection in the presence of: receiver collisions, ambiguous collisions, limited transmission, collusion power, false misbehaviour and partial dropping. • Depends only on Promiscuous listening. • Selfish nodes are just bypassed and not punished.	DSR
Path Rater	Increase in throughput with the increase in node mobility	Overhead in the transmission increases with increase the mobility	DSR
Sprite	• Cheat proof system • No requirement of any tamper proof hardware at any node	• Collusion attack • Difficulty in payment calculation • Message overhead	DSR
OCEAN	Distinguish the selfish and misleading nodes	No punishment	DSR
2ACK	• Checking of confidentiality of message • Increased packet delivery ratio • Scheme can be used with any source routing protocol.	• Message overhead • Chances for false positives • Traffic congestion	DSR/ AODV
SORI	• Computationally efficient as compared to other methods • It reduces the communication overhead	• Unable to differentiate between misbehaviour and selfish nodes • Has poor performance	DSR
CORE	• Good behaviour to be rewarded and bad behaviour to be punished. • Tolerable to sporadically bad behaviour, e.g. battery failure. • Nodes with bad reputation are isolated • Prevent DOS attacks • Impossible for a node to maliciously decrease another node's reputation	• Slow reaction. • Suffers from spoofing attack • It cannot prevent colluding nodes from distribute negative reputation	DSR
CONFIDANT	• Uses both direct and indirect observations from other nodes • No data forwarding service (punishment) is provided for low reputation nodes • Avoids possible bad routes	• Each node has different evaluations for same node to detect the selfish node • Eavesdropping is not addressed • Nodes in a black list are ignored. • Node authentication is not checked.	DSR

V. CONCLUSIONS

This paper has discussed various methods that deal with selfish nodes. Selfish nodes are a main problem for MANET as they affect the network throughput. Many approaches are proposed but no approach presented above provides a solid solution to the selfish nodes problem. With the said approaches selfish node still remains in network and enjoys services without cooperating with others and also we cannot eliminate all the selfish nodes from the network. A new method to reduce the effect of selfishness and encouraging the nodes to cooperate in the network services should be developed. These solutions must take into account some of the resource related limitations such as energy consumption and problem of reporting false positives. Selfish node detection methods should be integrated with existing MANET application with clear understanding of deployed applications and related attacks. Sometimes attack may be tried on detection system itself. Therefore, defense mechanism against such attacks should be considered carefully.

ACKNOWLEDGMENT

I would like to thank my guide Dr. B. D. Phulpagar for his timely support. Without his guidance it would have not been possible to complete this work. I would also like to extend my sincere thanks to Prof. Deipali Gore and Prof S. A. Itkar (Head of Computer Department) for continuous motivation to present this work.

REFERENCES

[1] R. Kaushik and J. Singhai, "Detection and Isolation of Reluctant Nodes using Reputation based Scheme in an Ad- hoc Network", International Journal of Computer Networks and Communications, vol.3, No.2, March-2011, pp. 95-105.

[2] S. Gupta1, C. Nagpal and C. Singla, "Impact of Selfish node Concentration in MANETs", International Journal of Wireless and Mobile Networks, vol. 3, No. 2, April- 2011, pp. 29-37.

[3] Dr, P. K. Suri et. al., "Exploring Selfish Trends of Malicious Mobile Devices in MANET", Journal of Telecommunications, vol. 2, No. 2, May-2010, pp. 25-29.

[4] L. Buttyan and J. Hubaux, "Nuglets: A Virtual Currency To Stimulate Cooperation In Self-Organized Ad Hoc Networks," Technical Report, Swiss Federal Institute of Technology, 2001.

[5] Y. Yoo, S. Ahn, and D.P. Agrawal, "A Credit-Payment Scheme for Packet Forwarding Fairnessin Mobile MANETs," IEEE ICC, 2005.

[6] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", IEEE Wireless Communications and Networking Confer- ence (WCNC), New Orleans, LA, March 2005.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks", International Conference on Mobile computing and Networking. New York, NY, USA: ACM Press, 2000, pp. 255–265.

[8] Buchegger S, Le Boudec J., "Performance analysis of the CONFIDANT protocol (Cooperation of Nodes Fairness in Dynamic Ad-Hoc Network)", ACM MobiHoc, 2002, pp 226–336.

[9] Michiardi P, Molva R., "Core: A Collaborative Reputation Mechanism To Enforce Node Cooperation In Mobile Ad Hoc Networks", International Conference on CMS, 2002. pp. 107-121.

[10] Bansal S, Baker M., "Observation-based cooperation enforcement in ad hoc networks", Technical Paper on Network and Internet Architecture, 2003.

[11] He. Q., Wu. D., Khosla. P., "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad- Hoc Networks", WCNC'04 IEEE Wireless Communications and Networking Conference, 2004.

[12] S. Zhong, J. Chen, and Y. Yang, "Sprite: A Simple, Cheat-Proof, Credit- Based System for Mobile Ad-Hoc Networks", Technical Report, Yale University, July 2002, pp. 1987-1997.

[13] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in Wireless MANETs", IEEE INFOCOM, 2003.

[14] Wei, Hung-Yu, Gitlin and Richard D., "Incentive mechanism design for selfish hybrid wireless relay networks," Mobile Networking and Applications, Vol. 10, No. 6, pp.929--937, Hingham, MA, USA, 2005.

