ISSN: 2321-7782 (Online)

Volume 3, Issue 2, February 2015

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Review Paper of Selfish Node Detection in MANET

Nikunjkumar Varnagar[1]
PG Scholar,
Computer Engineering, School of Engineering,
RK. University, Gujarat - India

Prof. Amit Lathigara[2]
Head of Department, Computer Engineering, School of Engineering,
RK. University, Gujarat - India

Abstract: Self-configuring, independent and decentralized without having a fixed infrastructure this kind of Network is known as Mobile Ad Hoc Network. Mobile nodes use the other nodes and trust them for transmitting data. Ad hoc networks have assumed that all nodes were cooperating. But, to save its resource an intermediate node may not cooperate for transmitting data to another node and saving resources. These nodes are known as selfish node. This could lead to degradation of network performance. In this paper, discusses behavior of selfish node, a survey of techniques used to detect selfishness attack in the network.

Keywords: MANET,DSDV, OLSR, WRP, AODV, DSR, TORA, ZRP, SHARP.

I. Introduction

In Mobile Ad Hoc Network [1] Consist of Mobile node which have capability to communicate with Each other using ireless link which can be direct or indirect. An Ad hoc network is a self-configuring system of mobile nodes. An Ad hoc network is an independent system where nodes are free to move within the network. MANETs decentralized and infrastructure less, therefore nodes are to move randomly and organize themselves arbitrary. Thus, the network's wireless topology may change rapidly. Topology changes are frequent and unpredictably in the network.

The rest of the paper is organized as follows: Section 2 MANET Routing Protocols, Behavior of Selfish node in section 3. In section 4, we conclude Different Techniques to detect selfish node. Comparative study discussed in section 5.

II. MANET Routing Protocol

Routing protocols define a set of rules which assign route from source to destination in a network. In ad hoc networks, topology is frequently changed, that's why nodes are not familiar with the topology of their networks. Each node learns about others nearby and how to reach them. In a MANET, there are three types of routing protocols [2]. A routing protocol is used according to the network situation.

2.1 Proactive Routing Protocols

Proactive routing protocols [3] are also called as a table driven routing protocols. In these protocols every node maintains a routing table which include information about the network topology even unless requiring it. The routing tables are updated periodically whenever the network topology changes because of the node are not fixed. Proactive protocols are not suitable for large networks because they need to maintain node entries for each and every node in the routing table of every node. Proactive protocols maintain a different number of routing tables varying from protocol to protocol. There are various routing protocols. Example: Destination-Sequenced Distance-Vector Routing (DSDV), Optimized Link State Routing Protocol (OLSR), Wireless Routing Protocol (WRP) etc.

2.2 Reactive Routing Protocols

A reactive routing protocol [4] is also known as on demand routing protocol. Reactive routing protocols do not make the nodes initiate a route discovery process until a route to a destination is required. In the Initial steps source node have to find route cache for the available route from source to destination if no route is available then node start the route discovery process. Each intermediate node involved in the route discovery process and adds latency. On demand routing protocols decrease the routing overhead but at the cost of increased latency in the network. These protocols are suitable in the situations where low routing overhead is required. Example of reactive routing protocols is: Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporarily Ordered Routing Algorithm (TORA) etc.

2.3 Hybrid Routing Protocol

Hybrid routing protocol [5] combines the advantages of proactive and reactive routing. Reactive protocols have less overhead and more latency while proactive protocols have large overhead and less latency. The hybrid routing protocol is a combination of both proactive and reactive routing protocols. So a Hybrid protocol covers the limitation of both proactive and reactive routing protocols. The hybrid routing protocol uses the route discovery mechanism of reactive protocol and the table maintenance mechanism of proactive protocol. Hybrid protocol is suitable for large networks where more numbers of nodes are present. This network is divided into a set of zones, where routing inside the zone is performed by using a reactive protocol and outside the zone routing is performed using reactive protocol. There are various hybrid routing protocols. Examples Zone Routing Protocol (ZRP), Sharp Hybrid Adaptive Routing Protocol (SHARP) etc.

III. Behaviour of Selfish Node

These nodes aim to get the greatest benefits from the networks while trying to preserve their own resources and use other node's resources, e.g. battery life or bandwidth. Selfish nodes attempt to maintain communications with the nodes it wants to send data packets to but may refuse to cooperate when it receives routing or data packets that it has no interest of cooperation in the network. Therefore, it may either drop data packets or refuse to retransmit routing packets that it has no interest in.

The selfish node can do the following possible actions[6] in Ad hoc network:

- When it receives a Route Request (RREQ), But Does not re-broadcast Route Request.
- Received Route Request (RREQ) but does not forward the Route Reply (RREP) on reverse route.
- Rebroadcast RREQ and forward RREP on a reverse route but does not forward data packets.
- Does not unicast Route Error (RERR) packets.
- Selectively drop data packets.

IV. Detection Techniques

There are various technique are used to detect selfish node attack in MANET. They are listed below.

4.1 Credit Based:

In credit based [7] approach introduce the concept of money and service charges. The natural idea is that nodes that used a service should be charged and nodes that provided a service should be remunerated. To this end, introduce a node currency that we call nuggets. Now, if a node wants to use a service (send a message), then it has to pay for it in nuggets. This motivates each node to increase its number of nuggets, because nuggets are necessary for using the network. Thus, the node is no longer interested in sending useless messages and overloading the network because this would decrease its number of nuggets, and it is better off providing services to other nodes because this is the only way to earn nuggets. If node’s nuggets reach at threshold value, node declares as misbehavior node.

4.2 Watchdog:

The watchdog [8] method allows detecting misbehaving nodes. When a node forwards a packet, the watchdog verifies that the next node in the path also forwards the packet. The watchdog listening to all other nodes within transmission range silently. If the next node does not forward the packet then it is tagged as misbehaved.

4.3 Pathrater:

The pathrater[9] (Rating of path), each node check possibility of every path in the network. Every node maintains a rating for every other node, it knows about the network. It computes a path metric by averaging the node ratings for the path. The calculation gives the overall reliability of different paths and allows accurate path in the network. If there are multiple paths to the same destination, path with the highest metric is more preferable.

4.4 Two Hop Acknowledgements:

In Two hop acknowledgment [10], detect misbehaving link instead of selfish node. TWOACK scheme detects misbehaving link and minimize the problem of routing misbehavior by notifying the routing protocol to avoid them for future reference. Detection of Misbehavior is dictated by sending back a TWOACK packet on successful acknowledgement of every data packet, which are assigned a fixed route of two hops (or three nodes) in the direction opposite to that of data packets.

4.5 Friends and Foes:

In Friends and Foes[11], It presents a long lived memory that allows nodes to be rewarded by services provided in the past but also does not charge by the number of hops used. The management of fairness by allowing nodes to publicly declare that they refuse to forward messages to some nodes. Every node maintains the following variables: friends, foes and selfish. The friends are the set of nodes to which node is willing to provide services. The foes are the set of nodes to which node is not willing to provide services and selfish variable gives the list of nodes which are known to act as if the node is a foe.

4.6 CONFIDANT:

CONFIDANT[12] (Cooperation of Nodes Fairness in Dynamic Ad-hoc Networks), has four interdependent modules monitor, reputation system, path manager and trust manager. First monitor collects evidence by monitoring the transmission of a neighbor after forwarding a packet to the next node in the route. Then reports to the reputation system only if the collected evidence represents a malicious behavior in the network. Reputation system changes the rating for a node if the evidence collected for a node's malicious behavior greater than the predefined threshold value. Then, path manager makes a decision to delete the malicious node from the path. Provide and accept routing information, accept a node as a part of route, and take part in a route originated by some other node this kind of Decision will take by Trust manager.

V. Comparative Study

TABLE 1 Comparative study

	Observation		Detection		Punishment
	Self to Neighbor	Neighbor to Neighbor	Selfish Node	Selfish Routing	
Credit Based	Yes	No	Yes	No	Yes
Watchdog	Yes	No	Yes	No	No
Pathrater	Yes	No	Yes	Yes	No
Two ACK	Yes	Yes	Yes	Yes	No
Friend and Foes	Yes	No	Yes	No	Yes
CONFIDANT	Yes	No	Yes	Yes	Yes

VI. CONCLUSION

Behavior of selfishness is appearing frequently in MANET. Due to the selfishness of node performance parameter were decreasing. In this survey paper we have discussed selfish node attack and different techniques related to detect selfish node. Due to a non co-operative of nature, the performance of the network is decreasing. Using this technique network performance will improve and easily detect selfish node in a mobile ad hoc network.

References

1. Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi "A Review of Routing Protocols for MobileAd-Hoc NETworks (MANET)" IJIET Vol. 3, No. 1, February 2013.
2. Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma Review of Various Routing Protocols for MANETs International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011.
3. T. Prasanna venkatesan , P. Rajakumar , A. Pitchaikkannu ,Overview of Proactive Routing Protocols in MANET International Conference on Communication Systems and Network Technologies, IEEE April 2014.
4. nand Nayyar Simulation Based Evaluation of Reactive Routing Protocol for MANET International Conference on Advanced Computing & Communication Technologies, IEEE January 2012.
5. S. R. Biradar, Hirenkumar Deva Sarma, Subir Kumar Sarakar, Puttamadappa C. Hybrid (Day- Night) Routing Protocol for Mobile Ad-Hoc Networks International Conference on Microwave Theory and applications, IEEE November 2008.
6. P. Sankareswary, R. Suganthi and G. Sumathi Impact of Selfish Nodes in Multicast Ad Hoc On demand Distance Vector Protocol International Conference on Wireless Communication and Sensor Computing , IEEE January 2010.
7. Levente Butty´an and Jean-Pierre Hubaux Enforcing Service Availability in Mobile Ad-Hoc WAN 1st Workshop on Mobile Ad Hoc Networking and Computing, IEEE 2000.
8. J. Hortelano, J. C. Cano, C. T. Calafate, and P. Manzoni Watchdog intrusion detection systems: Are They Feasible in MANETs? XXI Jornadas de Paralelismo, CEDI, Valencia, Spain, September 2010.
9. Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker Mitigating Routing Misbehavior in Mobile Ad Hoc Networks international conference on mobile computing and networking, Boston ,USA , August 2000.
10. Kashyap Balakrishnan , Jing Deng, Pramod K. Varshney TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks Wireless Communications and Networking Conference, IEEE March 2005.
11. Hugo Miranda, Luis Rodrigues Friends and Foes: Preventing Selfishness in Open Mobile Ad Hoc Networks International Conference on Distributed Computing Systems Workshops ,IEEE May 2003.
12. Sonja Buchegger , JeanYves Le Boudec Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Adhoc NeTworks) International Symposium on Mobile Ad Hoc Networking and Computing , Lausanne, Switzerland June 2002.