Impact on Performance Parameters in Mobile Ad hoc Network due to Selective Packet Dropping Attack

Bobby Sharma
Don Bosco College of Engineering and Technology
Assam Don Bosco University

Abstract- **Due to dynamic nature, capability to work in open medium, working capability without central server, Mobile Adhoc Network (MANET) becomes very popular amongst the users. Due to its flexibility, many times it is vulnerable to several kind of attack. Performance of MANETs always depends on co-operation of nodes in service providing. Main services provided by the nodes are to forward the packets to destination without creating hassles. But due to dynamic nature of the nodes, many times to save its resources, nodes show its selfish behavior by dropping the packets which are not intended for it. This misbehavior of nodes creates potential treats to the users. In this paper, Selfish behavior of nodes are analyzed by simulating the same using network simulator such as NS 2. Moreover, network throughput and packet delivery ration has been analysed by varying selfish node percentage, as well as by changing node mobility and pause time.**

Keyword: MANET, Selfish node, selective packet dropping, throughput, packet delivery ratio

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are a collection of mobile nodes that communicates over wireless media. According to Internet Engineering Task Force (IETF), MANET is an autonomous system of mobile routers (and associated hosts) connected by wireless links; the union of which forms an arbitrary graph **[13].**

A set of mobile hosts carry out the basic networking functions such as routing, packet forwarding, and service discovery. It doesn't require any pre installed infrastructure to establish the network. Nodes are self organized. These are free to move around. All the nodes in the network work as router as well as host at the same time **[14][15]16]**. Primary concern of the network is to maintain route traffic while connecting devices in MANET.

The topology of the network may change at any moment. Network may be partitioned in all the time. There is no fixed server. All the nodes in the network may work as client as well as host at the same moment. There is no fixed network infrastructure. Due to this dynamic nature, MANET is very popular amongst the user, but at the same time it suffers from vulnerabilities of attack. Behavior of MANETs is depended on the behavior of nodes. If the nodes perform their function well, efficiency of MANETs will also increase. But many times nodes show the misbehavior in several ways. Due to node mobility, they are very much concern with their resource savings. For this, some nodes don't route and forward the packets. In MANETs every node works as a router to share the information as well as to forward the packets due to limited range of radio transmission. In MANETs, nodes are concerned with battery power savings. From experiment it is clear that battery power consumption is higher in case of packet forwarding in comparison to packet receiving [1]. That is the reason why nodes are behaved selfishly to forward the packets to neighbor nodes while attaining services, which are meant for it from other nodes. As a result those selfish nodes don't show the cooperation in smooth running of the network. MANET forms the dynamic topography because of the mobile entities of the nodes. It has peer to peer (P2P) analogies and distributed approaches which results into share of common resources. Prevention are not enough to protect the network from misbehaving nodes like selfish node. Presence of selfish nodes in the network traps the network performance. In [9], it is mentioned that misbehavior activities are blocked by identifying their behavior. Selfish node decreases the whole data accessibility in the network. It affects the overall process of MANETs. In [10], it is mentioned that existence of selfish node in MANETs, affects the normal behavior of the network. Selfish nodes try to utilize the network resources for its own profit but reluctant to forward packets for other. It leads disruption of network and degrades network quality [11][12].

II. BEHAVIOR OF SELFISH NODES

In MANETs 80% of total energy of a node is consumed to forward the packets to other nodes. As a results, sometimes nodes don't show interest to forward packet which creates some serious problems in MANETs such as degradation of throughput, packet delivery ratio (PDR) or increase of end to end delay etc. Finally it leads to a serious threat known as selective packet dropping attack. Performance of the network in MANETs depends on the performance of the nodes. Generally a node in MANETs performs the following function:

- **Packet forwarding**: e.g. Source node sends some packets to destination via some hops in between whose main function is to forward the packets to next probable hop for reaching destination.
- **Routing**: Source node will discover a route to destination with the help of neighbor nodes.

A node may behave itself in several ways to show its malicious behavior. Out of which one of the behavior is selfish behavior of nodes. A selfish node behaves differently than the normal nodes that participated in network communication. The selfish behavior of a node in MANETs can be observed in following three ways:

1. Selfish nodes don't show interest to forward the data packet while they may forward the control packet. It forwards the control packet for route discovery, so based on this when other nodes try to send data packets, it simply drops all the data packets instead of forwarding them.
2. In this type of behavior, the selfish nodes stop themselves from forwarding any kind of packets. It is less harmful than the first one as nodes don't participate in routing
3. When the number of selfish nodes increase in a network, it degrades the network performance.

So, selfish nodes don't participate in routing, don't relay the routing data, set TTL value to a minimum possible value, modify the route request data, insert additional hop to consume more time, don't participate in current route, generate arbitrary RERR packets, don't send ACK packets, simply drop the packets which should be forwarded etc.[2] . Several solutions are suggested from several experiment to monitor the misbehavior of the nodes from its selfish behavior rely on watchdog technique [4]. Since a selfish host maintains a smaller back off interval with increasing chance of accessing the channel, thus reduce the throughput share attain by well-behaved station [5]. According to [6], a selfish node doesn't forward the data packet but may be agreed to forward control packets. It doesn't participate in route discovery. In another case it may observe its battery threshold and if it finds that the battery power of the nodes fall beyond the expected threshold, then the node starts misbehaving by simply dropping packets. Selective packet dropping attack is a kind of passive attack, nodes don't participate in network operation but not changing the packet content.

III. PARTICIPATION OF NODE IN PACKET FORWARD

In MANETs, nodes must be responsible for forwarding the packet instead of keeping itself silent. Due to node mobility, the communication range in between the nodes may change at any moment. In such condition nodes should act itself as router and must take part in route discovery for packet forwarding. But sometimes selfish node doesn't participate in route discovery phase. As a result, forwarding function for all incoming packets is stopped [6]. Similarly they show less interest to maintain number of hops to reach destination, sequence number of packets etc [7]. To maintain all these parameters by node, the node has to utilize its memory, CPU cycle, bandwidth and most importantly the battery power, so the node expose its selfish behavior by simply dropping the packets without acknowledging it to source.

IV. ROUTING PROTOCOL

To compute the performance of nodes or to observe the selfishness of nodes in MANETS, one must be aware about the routing protocols of MANETs.

The broad classification of MANETs protocols may be identified as follows [8]:

Proactive Protocol

a. Link State

OLSR: Optimized link state protocol
OSPF

b. Reactive
DSDV: Destination sequence distance vector

Reactive Protocol
DSR : Dynamic source routing
AODV: On demand distance vector

Hybrid Protocol
ZRP: Zone routing protocol
TORA: Temporary ordered routing protocol

In proactive protocol, MANET routing information need to maintain constantly. The whole network should be understood by all nodes. This results in a constant transparency of routing traffic; there is no initial delay in communication.
Reactive protocols set up the routes on-demand. If a node wants to setup communication with a node to which it has no route, the routing protocol will try to establish such a route.

For simulation purpose, reactive protocol AODV is used because in case of reactive protocol, the network seeks to set up routes on demand. AODV uses Dynamic Routing Table and Bellman-Ford algorithm [8], If a node wants to communicate with a node to which it has no route, the routing protocol will try to establish a route. In case of AODV, the information related to path of data transmission is relayed on demand only. It will generate a route request (RREQ) when a node wants to communicate with another node in which it has no route. A route is considered found when the RREQ message reaches either the destination itself, or an intermediate node with a valid route entry for the destination. If due to some reason route becomes invalid, AODV will again issue a RREQ. Similarly it uses another two messages like RREP and RERR in response to Route reply and route error. Moreover AODV maintains times based states in each node for maintaining utilization of individual routing table entries. AODV also inform all the nodes using link when a failure occurs in particular points due to some reasons [7].

V. SIMULATION ENVIRONMENT

For simulation, NS 2 is used. Simulation environment is shown in Table 1.

Table 1: Simulation Environment

Animation area	1000m X 1000m
Mobility model	Random way point
Channel type	Wireless
No. of nodes	50
Simulation time	300 sec
Pause time	10-70 sec
Node Speed	10-70 m/s
Data rate	100 kbps
Transmission range	100 m
Packet size	512 byte
Traffic type	CBR
Routing protocol	AODV

Two performance parameters such as Packet Delivery Ratio (PDR) and Throughput of the network are used tomeasure the affect of selfish node in the network. Performance is evaluated for increasing number of selfish nodes, increasing order of node mobility with certain number of selfish node and pause time. Then increasing order of pause time with fixed number of selfish node and node mobility. Relevent graphs are as follows,

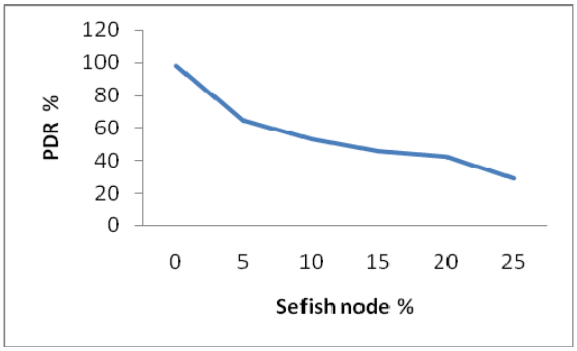

Figure 1: PDR variance with increasing order of Selfish node

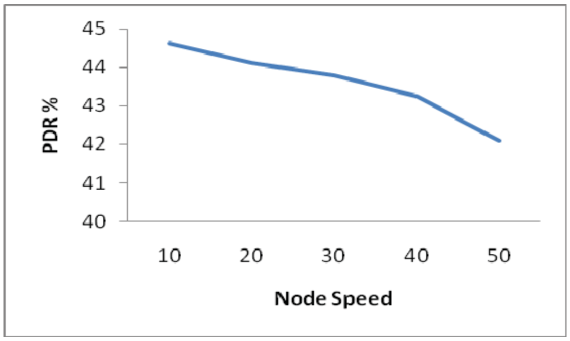

Figure 2: PDR variance with increasing order of node mobility

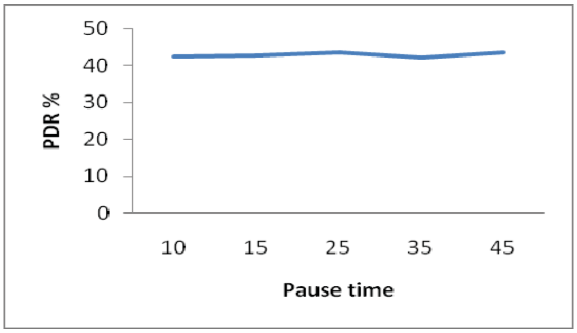

Figure 3: PDR variance with increasing order of Pause time

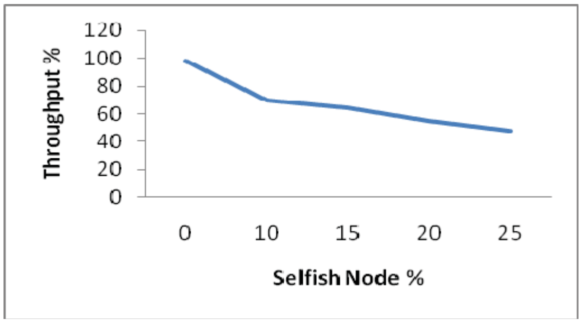

Figure 4: Throughput (%) variance with increasing order of Selfish node

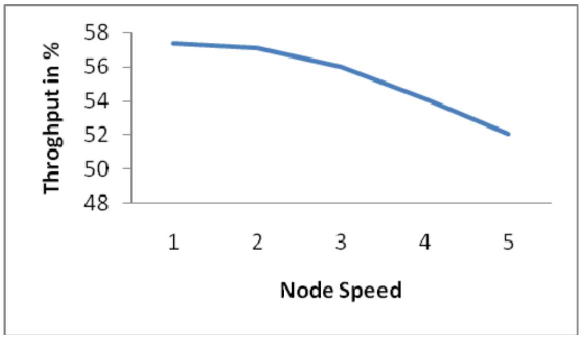

Figure 5: Throughput (%) variance with increasing order of node mobility

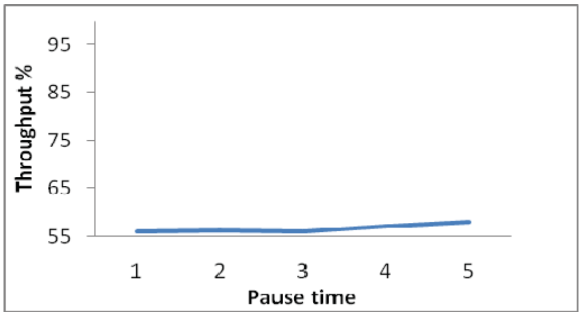

Figure 6: Throughput (%) variance with increasing order of pause time

VI. OBSERVATION

In Figure 1, when the percentage of selfish nodes is increasing, throughput in the network is gradually decreasing for AODV. Since throughput of the network depends on number of delivered packets and selfish nodes do not forward the packets to its neighbor nodes, so increasing number of selfish nodes in the network will deliberately decrease the throughput of the network.

In Figure 2, it is observed that as node mobility is increasing with fixed number of selfish nodes, throughput is degrading gradually in AODV. It is because of the fact that due to high node mobility, node will lose the connection repeatedly and reinitiate the route between source and destination. As a result some packets are also dropped in addition to selfish behavior of nodes in the network.

In Figure 3, it is observed that when the network contains constant number of selfish nodes and pause time of the network is gradually increasing, the throughput of the network comes down to certain level and it almost maintains the constant level. It is because of the fact that high pause time implies more stable network, so there is very less number of extra packet lost except the lost due to selfish nodes.

In Figure 4, PDR is decreasing with increased number of selfish nodes as selfish nodes invariably drop packets or not forwarding the packets. Moreover, AODV is not capable of resisting the selfish node behaviour in the network. When the percentage of malicious nodes is increasing then PDR is falling down due to network's non scalability and non capability to detect selfish node dynamically. Due to dynamic nature of MANETs, nodes may change their status, they may quit from the range, then they again come to the range with different IP.

In Figure 5, with increase node mobility, the network with constant number of selfish nodes, further makes PDR unstable. Since high node mobility makes the network unstable. That leads to instability in the network performance parameters.

In Figure 6, though the pause time increasing gradually, it doesnot affect PDR much. It is because of the fact that existence of selfish nodes in the network, doesnot allow the network to deliver packets to destination. Instead of that it selectively drops packets.

VII. CONCLUSION

In this paper various causes and behavior of selfish nodes in MANETs has been analysed along with different routing protocol. It is also analysed that performance of MANETs depends on node's cooperation in packet forwarding. Affect of selfish nodes in MANETs are analysed for two main performance parameters such as network throughput and packet delivery ratio for the protocol AODV. Simulation is done for increased number of selfish node as well as network with increase node mobility and pause time with constant number of selfish nodes.

REFERENCES

[1] Yongwei, Wang, Venkata C. Giruka and Mukesh Singhai, "A Fair Distributed Solution for Selfish Nodes Problem in Wireless Ad Hoc Networks" , Springer Berlin / Heidelberg, 0302-9743 (Print) 1611-3349 (Online), Volume 3158/2004, pages 630, 10.1007/b99253, 2004, 978-3-540-22543-0

[2] Djamel Djenouri and Nadjib Badache, "MANET: Selfish Behavior on Packet Forwarding", Encyclopedia of Wireless and Mobile Communication, DOI: 10.1081/E-EWMC-120043599 Copyright @ 2008 by Taylor & Francis.

[3] Frank Kargl, Andreas Klenk, Stefan Schlott and Michael Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks", Springer Berlin / Heidelberg, Springer Berlin / Heidelberg, Volume 3313/2005, pages 152-165, Security in Ad-hoc and Sensor Networks, 10.1007/b105219

[4] Djamel Djenouri and Nadjib Badache, "New Approach for Selfish Nodes Detection in Mobile Adhoc Networks", 0-7803-9469-0/05/$20.00 @2005 IEEE, Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005, Publication Date: 5-9 Sept. 2005, page(s): 288- 294, ISBN: 0-7803-9468-2, INSPEC Accession Number: 9027006, Digital Object Identifier: 10.1109/SECC MW.2005.1588323

[5] Lei Guang and Chadi Assi, Abderrahim Benslimane, "Modelling and Analysis of Predictable Random Backoff in Selfish Environment", MSWiM'06, October 2-6, 2006, Terromolinos, Malaga Spain. Copyright 2006 ACM 1-59593-477-4/06/0010.

[6] Djamel Djenouri and Nadjib Badache, "Selfishness: an emergent threat on Packet forwarding in Mobile Adhoc Networks"

[7] Samyak Shah1, Amit Khandre2, Mahesh Shirole3 and Girish Bhole, "Performance Evcaluation of Ad Hoc Routing Protocols using NS2 Simulator", Mobile and Pervasive Computing (CoMPC-2008)

[8] Giancarlo Pellegrino, "Security Analysis of MANET in NS2", Mini Workshop on Security Framework 2006, catania, December 12,2006

[9] Gaurav Soni and Kamlesh Chandrawanshi, "A NOVEL DEFENCE SCHEME AGAINST SELFISH NODE ATTACK IN MANET," International Journal on Computational Sciences & Applications (IJCSA) Vol.3, No.3, June 2013

[10] N.R.Suganya and S.Madhu Priya, "Detecting Selfish Nodes in a MANET through Fragmentation in Distributed Environment ," International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, No 6, June 2013, ISSN: 2278 – 7798

[11] Shailender Gupta, C. K. Nagpal and Charu Singla "IMPACT OF SELFISH NODE CONCENTRATION IN MANETS," International Journal of Wireless & Mobile Networks (IJWMN, 2011) Vol. 3, No. 2

[12] Kiran, Kumar Sanjay and Patle V. K , "Effect of Selfish Nodes in Trust Base Route: MANET," Research Journal of Science and Technology 2013, Vol 5, Issue:3, page(s):327-330, Print ISSN : 0975-4393

[13] Lakshmi P.S., Pasha Sajid2 and Ramana M.V, "Security and Energy efficiency in Ad Hoc Networks," Research Journal of Computer and Information Technology Sciences 2013, Vol. 1(1), page(s): 14-17

[14] Chun-Ta Li,"A secure routing protocol with node selfishness resistance in MANETs," Int. J. Mobile Communications, Vol. 10, No. 1, 2012 103

[15] Praveen Joshi, "Security issues in routing protocols in MANETs at network layer," World Conference on Information Technology, 2011, Vol. 3, Page(s): 954–960

[16] Shakshuki, E.M., Nan Kang and Sheltami, T.R., "Intrusion-Detection System EAACK—A Secure for MANETs," Industrial Electronics, IEEE Transa-ctions on March 2013, Vol. 60 , Issue: 3, Page(s):1089 – 1098, ISSN :0278-0046