IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

An Effect of Selfish Nodes on Network Performance in MANET

Ms. Lilu Odedra[1], Prof. Ashish Revar [2], Prof. Munindra H. Lunagaria [3]

PG Scholar, Department of Computer Engineering, Faculty of PG studies-MEFGI, Rajkot, India [1]

Assistant Professor, Department of Computer Engineering, Faculty of PG studies-MEFGI, Rajkot, India [2]

Assistant Professor, Department of Computer Engineering, Faculty of PG studies-MEFGI, Rajkot, India [3]

Abstract: Mobile Ad-hoc Network(MANET) is the infrastructure less and the central object less network in which the mobile nodes can be communicate with the wireless connections. Any node can join and leave the network anytime nodes may change its place and move one place to another place anytime in network. Due to this characteristics of MANET it's a more vulnerable to network attacks such as black hole, gray hole, sink hole and selfish attacks. The aim of the selfish attack is to preserve the own resources such as battery power, bandwidth etc. This paper surveys the effect of selfish attack on the network performance matrices.

Keywords: Network Security, MANET, Selfish attack, countermeasures, wireless security, Types of selfish attack;

I. INTRODUCTION

MANET is the self-organized network in which any node is free to join and leave network. In the MANET there is three types of routing protocols 1) reactive 2) proactive and 3) hybrid. The reactive protocol is on-demand protocol in this route discovery is established whenever routing is needed. This types of protocols are AODV, DSR [1] [3] etc. The proactive protocols are the table driven protocols in which each nodes route information is stored before the route discovery. Whenever the route needed the path is retrieved from routing table i.e. OLSR, DSDV [4] [2] etc. The hybrid protocol uses properties of both proactive and reactive protocols I.e. ZRP, TORA [5]. In the MANET various attacks are influence the routing due to its non-infrastructure architecture. Any unauthenticated node is join the network easily and violet the network communication. There is mainly two types of attacks are there one is the active attack and another is passive attack. In the active attack the intruder node can be unauthorized access and modified the data over the network i.e. denial of service, black hole attack, gray hole attack etc. on the other end in the passive attack the intruder node only observe the communication over the source and destination and get the important information but did not alter the data i.e. wiretapping, port scanner etc. In the MANET the mostly attacks are performed on the AODV protocol because it less secure to attacks. The attacks are the black hole, wormhole and selfish attacks which all are the type of denial of service.

This paper focus on the selfish attack which is one of the type of denials of service attack. In the network node will be act as selfish and does not forward the packets of other node towards to save its network resources for own transmission. There is many type of selfishness i.e. MAC selfish behavior, packet dropper misbehavior, partial dropping, false accusations misbehavior, set TTL field to zero misbehavior, insufficient transmission power selfishness. The reason for the node selfishness is to save own resources like energy, storage space, CPU cycles, network bandwidth etc.

The rest of the paper will be organize following section (II) Types of the selfish behaviors (III) Related work (IV) AODV protocol V) Performance Matrix VI) Simulation Setup VII) Results & Discussions VIII) Conclusion

II. TYPES OF SELFISH BEHAVIOURS

The various selfish behaviors are performed by the selfish nodes by not forwarding data of other nodes, which all are described as below.

1. Forwarding Node Selfish Behavior

The selfish node does not forward the packets of other nodes to save its resources. As shown in the analysis of Abdelaziz Babakhouya et al. [6] Selfish node may decide to do not consume their resource in forwarding data packets for other. Based on author's simulation packet data fraction (PDF) is same as the high and low density of nodes and Percentage of selfish node increase the end-to-end delay is increased.

2. MAC layer Selfish Behaviors

The selfish node misuses the MAC protocol to gain more network resources than well behaves node through that it obtain large portion of channel and capacity to improve its throughput. Lei Guang et al. [7] observe that Selfish node choose smaller back off interval, thereby increasing its accessing channel capacity and hence reduce the throughput share received by well-behaved nodes.

3. Set TTL field to zero misbehavior

Hyun Jin Kim et al. [8] state that selfish nodes drop routing packets or forward with at Time to live (TTL) of 0 so that no path can be establish also type of artificially increasing hop count type behavior in which the node behaving

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

selfishly seems longer than they really are, so node likely don't choose that path.

4. Disobey the Protocol Specification rules to get higher throughput

R.Gunasekaran et al. [9] Stated that nodes can deviate from the protocol specification in order to obtain a given goal, at expense of honest participants and disobey the rules for access the wireless channel in order to obtain higher throughput than other nodes it is by back off manipulation, shorter DIFS and oversize NAV.

5. Network card on/off selfish behaviors

Hemang Kothari et al. [10] stated that in network card on/off selfish behavior the node refusing to forward any control or data packets for others by Turn off the power of network card or by Turn off the communication function when they do not need to communicate. Authors stated that this behavior saves more energy than the other selfish behaviors.

6. Partial Dropping Misbehavior

Djamel DJENOURI et al. [11] shows that in watchdog mechanism node can't be detected as wrong by dropping packets at lower rate than watchdog's configured minimum misbehavior threshold.

7. False Accusation misbehavior

Djamel DJENOURI et al. [11] Shows that the node may falsely accuse the legitimated node by adjusting the transmission power. The selfish node keeps its transmission power more toward source node and less toward adjacent node and do not forward packets to its adjacent node so source can't hear transmission of next node of selfish node and selfish node falsely accused a legitimated node as selfish.

8. Link Breakage Selfish Behavior

In Wei Yu and K.J. Ray Liu [12] selfish node silent about the link breakage in path and do not inform to source, so it wastes other node's energy and put down all of nodes into the starvation.

III. RELATED WORK

The authors Hemang Kothari et al. [10] simulate two selfish behaviors namely forwarding node selfish behavior and network card on/off selfish behavior using DSR. They compare the energy saving to the selfish nodes for both the misbehavior's and show that network card on/off selfish behavior saves more energy.

Secondly, with their simulation study they find that in dense mobile ad hoc networks where route breakages are frequent, routing control packets consumes significant fraction of node energy and selfish behavior by certain number of nodes reduce the overall routing overhead in network which in turn result in energy saving for both, well behaving nodes and selfish nodes.

Abdelaziz Babakhouya et al. [6] studied the misbehaving nodes impact on MANET performance with DSR routing protocol simulate two types of selfish behaviors, Dropping RREQ and Data dropping. With simulation, authors find that Selfish node type of dropping RREQ don't cause any damage in network with high nodes density. However, it can really affect the end to end delay and lead to congestion in a low density network. One malicious node carrying a black hole attack can have the same effect as 20% to 30% of selfish nodes type of Data dropping misbehavior. Rooshabh.H.Kothari et al. [13] proposed an Enhanced DSR Routing by using selfish nodes in network, and they found from results that enhanced DSR routing protocol is better than existing DSR protocol on performance measures such as throughput, routing overhead, end to end delay and packet delivery ratio.

It has been found that on dense network certain numbers of selfish nodes are supportive to reducing communication overhead.P. Sankareswary et al. [14] proposed a Multicast ad-hoc on demand distance vector protocol for detecting selfish nodes in MANET. It uses the two-hop acknowledgment scheme for detecting selfish nodes and redundancy bit mechanism is provided to recover selectively dropped packets. The performance evaluation shows the effect of selfish nodes on performance matrix for with attack and after providing secure solution. After providing secure solution the performance matrices is increased.R Kaushik et al. [15] evaluate the packet dropping selfish behavior in the implementation study and detect selfish nodes which are created due to nodes conserving their energy. After their detection, performance analysis of networks has been carried by comparing the ideal network and the network with selfish node using NS2. Simulations shows that the network performance is degraded when selfish nodes are there.

IV. AODV PROTOCOL

The Ad hoc On-demand Distance Vector (AODV) [16] routing protocol is a simple and efficient reactive routing protocol, based on the distance vector approach. It is designed specifically for use in multi-hop wireless MANET scenario. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on demand. When a node S wants to send a packet to another node D, the source node S performs a Route Discovery by broadcasting a ROUTE REQUEST (RREQ) packet to the destination node D, which is flooded throughout the network in a controlled manner. A ROUTE REPLY (RREP) packet is unicasted to S from either the destination node D, or another intermediate node that knows a route to D. Every node forwarding the RREQ message caches a route back to the source node S.

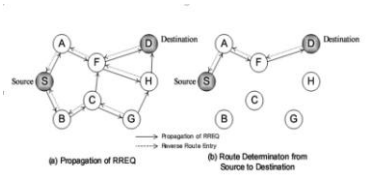

Fig 1: AODV Routing Protocol

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Routes are maintained by using ROUTE ERROR (RERR) message, which is sent to notify other nodes about a link breakage. HELLO messages are used by the nodes for detecting and monitoring links to their corresponding neighbors.

V. PERFORMANCE MATRICES

The following are the performance matrices which we are going to measure for show effect of selfish nodes on networks.

1. Packet Delivery Ratio

It is the percentage of total number of packets received by the intended receivers to the total number of packets originated by all nodes.

2. Throughput

Throughput or network throughput is the average rate of successful message delivery over a network. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

3. Goodput

Goodput is the average rate of successful data packets delivery over a network.it only consider data packets and it is the ratio of forwarded packets without control packets. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

VI. SIMULATION SETUPS

The simulation was done using the NS-2. Simulator [16], which provides a salable simulation environment for wireless networks. In order to measure the impact of selfish nodes in ad hoc network performances, the AODV implementation was modified using the NS-2 simulator. Table I represents the simulation parameters along with their corresponding values. The simulated network consists of 25,50,75,100 nodes placed randomly in 500x500 areas and we are performing evaluation with varying selfish nodes i.e. 2,4,6,8. Each node moves at a speed of 4.0 m/s.

The CBR file and Scenario is generated with following commands in ns 2.35.

- ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] –seed seed] [-mc connections] [-rate rate] > cbr_filename
- ./setdest [-n num_of_nodes] [-p pausetime] [-s maxspeed] [-t simtime] [-X maxx] [-Y maxx] > scen_filename

VII. RESULTS & DISCUSSIONS

In this section the experimental results is shown for selfish nodes performance of AODV routing, important Performance Parameters are analyzed by varying no. of nodes and no. of selfish nodes.

1. THROUGHPUT

As shown in the graphs for various no. of nodes the throughput is decreased as increase in no. of selfish nodes. The selfish nodes drop the routing packets of other nodes and the average throughput of the network is decrease with increase the no of selfish nodes.

arameter	Value
Simulator	NS-2.35
Protocol	AODV
Simulation Time	150s
No of Mobile Nodes	25,50,75,100
Area	500x500
Traffic Type	CBR
No of Selfish Nodes	0,2,4,6,8
No of. Connections	20

Table I Simulation Parameters

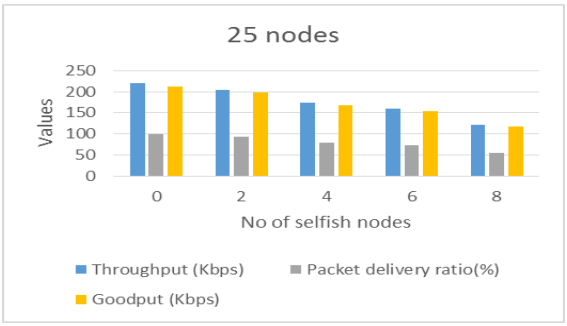

Fig-2 Throughput, Packet Delivery Ratio, Good put for 25 nodes.

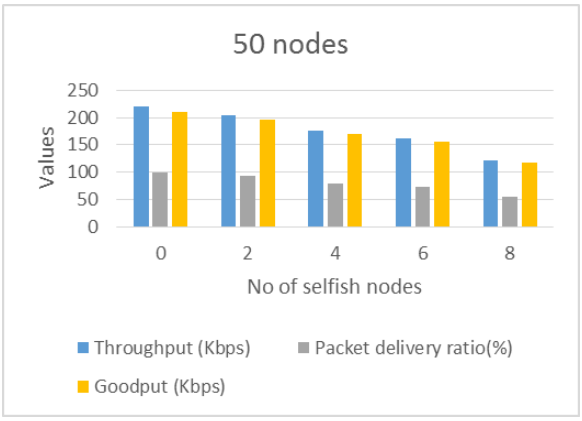

Fig-3 Throughput, Packet Delivery Ratio, Good put for 50 nodes.

Fig-4 Throughput, Packet Delivery Ratio, Good put for 75 nodes.

2. GOODPUT

As shown in the Figures, the packet Goodput of network is decreased as increase the no. of selfish nodes.it is network throughput without the control packets, its only consist data packets. Compare to absence of selfish nodes, when there is a presence of selfish nodes the Goodput is decreased and also results shows that when we increase the selfish nodes it will decrease the Network Performance.

DOI 10.17148/IJARCCE.2016.5625

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

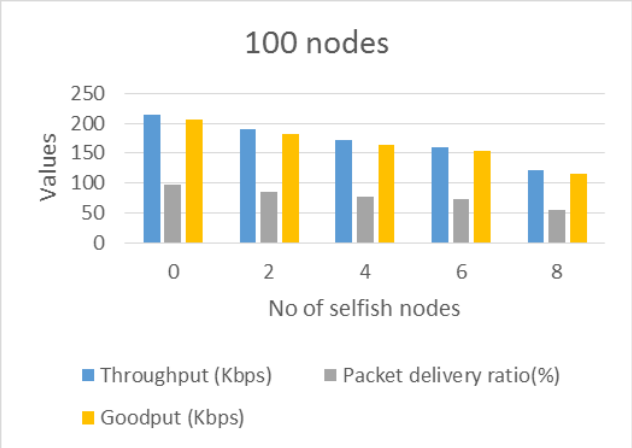

Fig-5 Throughput, Packet Delivery Ratio, Good put for 100 nodes

3. PACKET DELIVERY RATIO

As shown in the Figures, the packet delivery ratio of network is decreased as increase the no. of selfish nodes.in this 0 indicates absence of selfish nodes. Compare to this when there is a presence of selfish nodes the Packet Delivery Ratio is decreased and also results shows that when we increase the selfish nodes it will decrease the Network Performance.

VIII. CONCLUSION

In this paper, the simulation of AODV Protocol under without selfish attack and with selfish attack has been carried out using NS-2.35 simulator. Simulation has been done for 25, 50, 75, and 100 nodes in ad hoc network and 0(no selfish nodes), 2, 4, 6 and 8 selfish nodes. It has been analyzed both protocols in terms of throughput, Packet Delivery Ratio and Goodput. If we include concept of selfish behavior node in AODV protocol then in enhanced version of protocol, the results of simulation show that this has far above the ground effect on AODV protocol. From the simulation results and as shown in graphs that if we include selfish behavior node in AODV protocol then there is significant decrement Throughput which indicates selfish nodes drops the packets and it will result in network degradation. Packet delivery ratio is decreased as increase in no. of selfish nodes.Goodput is decreased as increase in no. of selfish attack. From this paper it has been concluded that increasing a no. of nodes does not much effect on the network performance with selfish nodes. During this attack selfish node tends to drop route request packets which intern improve network performance, reduces collision and saving resources for whole network. In a way density always reduce the effect of attack because more no. of good nodes will do more work to solve problem.

REFERENCES

[1] Shao, Baohua. "Performance of Ad Hoc on Demand Distance Vector Routing Protocol." In 2010 International Conference of Information Science and Management Engineering, pp. 420-421. IEEE, 2010.

[2] Mahdipour, Ebrahim, Amir Masoud Rahmani, and Ehsan Aminian. "Performance evaluation of destination-sequenced distance-vector (dsdv) routing protocol." In Future Networks, 2009 International Conference on, pp. 186-190. IEEE, 2009.

[3] J. Broch. D. B. Johnson, and D. A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," IETF Internet draft, draft-ietf- manet-dsr-01 txt, Dec. 1998

[4] Hilippe Jacquet, Paul Muhlethaler, Amir Qayyum, Anis Laouiti, Laurent Viennot and Thomas Heide Clausen "Optimized Link-State Routing Protocol", draft-ieft-ols r-04.txt - March 2001

[5] A.vani." Study of MANET Routing Protocols TORA, LDR, ZRP." International Research Journal of Engineering and Technology (IRJET) on, pp. 1889-1891. vol-2,issue-3(2015).

[6] Babakhouya, Abdelaziz, Yacine Challal, and Abdelmadjid Bouabdallah. "A simulation analysis of routing misbehaviour in mobile ad hoc networks." In Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST'08. The Second International Conference on, pp. 592-597. IEEE, 2008.

[7] Guang, Lei, and Chadi Assi. "Mitigating smart selfish MAC layer misbehavior in ad hoc networks." In Wireless and Mobile Computing, Networking and Communications, 2006.(WiMob'2006). IEEE International Conference on, pp. 116-123. IEEE, 2006.

[8] Kim, Hyun Jin, and Jon M. Peha. "Detecting selfish behavior in a cooperative commons." In New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on, pp. 1-12. IEEE, 2008.

[9] Gunasekaran, R., V. Rhymend Uthariaraj, R. Sudharsan, S. Sujitha Priyadarshini, and U. Yamini. "Detection and prevention of selfish and misbehaving nodes at MAC layer in mobile ad hoc networks." In Electrical and Computer Engineering, 2008. CCECE 2008. Canadian Conference on, pp. 001945-001948. IEEE, 2008.

[10] Kothari, Hemang, and Manish Chaturvedi. "Effect of Selfish Behavior on Power Consumption in Mobile Ad Hoc Network." Proceedings of the Asia-Pacific Advanced Network 32 (2011): 91-100.

[11] Djenouri, Djamel, and Nadjib Badache. Two hops ack: A new approach for selfish nodes detection in mobile ad hoc networks. Technical report LSI-TRO704, University of Scinece and technology houari boumediene, Algiers, Algeria, 2003.

[12] Yu, Wei, and K. J. Liu. "Attack-resistant cooperation stimulation in autonomous ad hoc networks." Selected Areas in Communications, IEEE Journal on 23, no. 12 (2005): 2260-2271.

[13] Kothari, Rooshabh, and Deepak Dembla. "Modeling, Implementation and Performance Analysis of Selfish Behavior in Enhanced Selfish-DSR Routing Protocol of MANET." International Journal of Computer Applications 66, no. 23 (2013).

[14] Sankareswary, P., R. Suganthi, and G. Sumathi. "Impact of selfish nodes in multicast Ad hoc on demand Distance Vector Protocol." In Wireless Communication and Sensor Computing, 2010. ICWCSC 2010. International Conference on, pp. 1-6. IEEE, 2010.

[15] Rekha Kaushik, Dr. Jyoti Singhai, "Simulation Analysis of Node Misbehavior in an Ad-hoc Network using NS2", International Journal of Computer Science and Information Security (IJCSIS), Vol. 8, No. 4, July 2010

[16] Mubashir Husain Rehmani,Sidney Doria, and Mustapha Reda Senouci " A Tutorial on the Implementation of Ad-hoc On Demand Distance Vector (AODV) Protocol in Network Simulator (NS-2)" June 2009