IMPACT OF SELFISH NODES ON MOBILE ADHOC NETWORK

SUJETHIRA. A,

PG scholar Department of IT, Sona College of Technology,Tamilnadu,India.

sujethira@yahoo.in

ABSTRACT-*A MANET (Mobile Adhoc Network) is an infrastructure-less network that consists of mobile nodes which voluntarily co-operate with each other to perform an operation. Some of the mobile nodes deviate from this behavior and the nodes want to conserve it energy without participating in the network operation. Thus these nodes are regarded as selfish nodes and this term is referred as selfish node behavior in the network. Watchdog is one of the mechanisms in detecting these selfish nodes. The watchdog produces false positive and false negative leading to wrong operations. The CoCoWa method is based on the diffusion of the false positive and false negative events when a contact occurs and so the detection time is reduced along with the increase in precision. This work aims at the comparison of the network performance by incrementing the selfish node count and evaluation of the results is shown by parameters.*

Keywords:**MANET, watchdog, CoCoWa.**

1. INTRODUCTION:

The MANETs has independent mobile nodes that communicate with each other through radio waves. These nodes communicate with each other directly when they are in radio range while others have intermediate nodes to route the packets. The characteristics of the Mobile Ad-hoc Network are dynamic topology, light weight terminal, shared physical medium, multihop routing, and distributed operation. While using MANET we get several advantages and they are self-configuring, scalable, independent of geographic position, less expensive, flexible and robust. Many numbers of nodes can be added to the network so it is scalable and flexible to any number of changes in the topology. Robustness is because of decentralized administration. Unlike the advantages there are some disadvantages that is exhibited by the network. The bandwidth is limited for the nodes. The dynamic topology causes the battery to drain its power sooner. A hidden terminal problem occurs which is formed due to the collision of nodes.

Unnecessary routing overhead are formed in the routing table. When a transmission error occurs the packets are lossed which is disadvantage and leads to the frequent route changes. The security threats are the major problems to be handled correctly in the network if not the network is collapsed totally or they are insecure. The CoCoWa(Collaborative Contact based Watchdog)deals with the attacks in the data link layer. There are mobile nodes which don't cooperate with other mobile nodes. This type of behavior is known as selfish node behavior because those nodes do not share the packets once they receive it. There is a mechanism to detect these type of nodes and it is known as watchdog mechanism. The watchdog even though it detects the selfish nodes, it suffers from two problems. They are false positive and false negative events generation. These events are generated when watchdog detects the network they reduces the effectiveness of the mechanism. It is shown that the packet loss number is increased by 500% when the selfish node ratio increases from 0 to 40% [1]. The overall performance of the network such as average hop count, throughput, ratio of packets delivered is seriously affected and degraded [2].

2. LITERATURE REVIEW:

A) Self-Policing Mobile Ad-Hoc Networks by Reputation Systems:

The degradation of the mobile ad-hoc network performance is caused due to the misbehavior of nodes such as selfishness or faulty nature or malicious reason. The misbehavior in self-organized network can be managed by changing the level of co-operation between them. The self-policing mechanism with reputation method is made to function the misbehaving nodes even though it has some problem. All the nodes consist of its own reputation system and perform detection by observing them and using second hand information. Whenever a misbehaving node is found it is isolated from the network. The classification of the reputation system features and also the use of second hand information are included here [7]. The second hand information will not be considered when misbehaving nodes surround a normal node. Here the co-operation is not guaranteed because there is no benign alternative for first hop of a route.

B) Watchdogs for intrusion detection system in VANET:

The usefulness of watchdog for intrusion detection is evaluated in VANET (Vehicular AdhocNETwork). It consists of three fold components [3]. First component is to support all kind of routing protocols thus making protocol independent. The second is to provide high detection coverage along with low detection latency. Final

component is to minimize false positive and false negative. The result is to obtain the balance between coverage and detection latency of watchdog. Tolerance threshold and devaluation are the two mechanisms included here. The watchdog is vulnerable two consecutive malicious attacks and it is a disadvantage. The tolerance threshold is not dynamic which is not suitable for all.

C) CORE Watchdog Mechanism in Mobile Ad Hoc Networks:

CORE mechanism is a mechanism that extends the basic network functions like network management, packet forwarding etc. CORE (Collaborative REputation) is based on Dynamic Source Routing (DSR) protocol which is an 'on demand' protocol [6]. It allows a node to 'dynamically' discover a route to any other node in the network for which it has no path. The collaborative monitoring technique is used in the CORE's reputation scheme. Every member of the network uses reputation technique to store information about an entity's contribution to the network operations. The reputation is a measure of rate of collaboration of an entity. The CORE gathers the reputation information in three ways such as subjective reputation, indirect reputation and functional reputation. The subjective reputation is calculated when a node observes other nodes activity and it gives more relevant information from the past data. When indirect reputation is considered it provides information from other community members. Thus finally the functional reputation calculates with respect to different function f. The CORE paper explores the working components and analyze the watchdog mechanism with the help of two functions namely DSR route discovery and forwarding the packet when the mechanism.

3. PROPOSED WORK:

The analysis has been done and the results are compared when the network exhibits selfish node behavior. The wireless network has large number of security threats than wired networks because it communicates using broadcast messages. Hence there will be no assurance of the data security.

MANET is also a kind of wireless network which has many misbehaviors in its network. One of the types is selfish node behavior. Here the nodes exhibit the misbehavior within the network. Whenever a packet is sent to destination from source it has to reach through some intermediate nodes. Those intermediate should forward the packet properly in order to reach the receiver but there may be nodes which receive packet from its preceding node and do not send it to the proceeding node. This action is performed either to conserve its own energy or drop packets and it is known as selfish behavior.

The selfish behavior affects the transmission of the data in the whole network seriously. The work is related to the impact of these selfish node behaviors and it has been checked with parameters using x-graph. The number of normal nodes and selfish node count has been increased to verify the performance of the network. The simulation results are plotted using graph for better clarity.

4. SIMULATION AND RESULT:

4.1. Simulation environment:

Simulation is a powerful tool as it gives a way for alternative designs and plans can be calculated without any experiment on a real system which may cost high, consumes time and impractical to do. Network simulator is software used for depicting simulation. There are several types of simulators such as NS2, GloMoSim, TOSSIM, NetSim, OPNET etc.

Among these simulators in this paper NS-2 is used which is an open source software. It has been chosen because the programming is done using OTCL and also protocol simulation is easy in it for wireless adhoc network.

4.2. Analysis using parameters:

4.2.1. Packet delivery ratio:

The ratio of the packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

$$PDR=\frac{number\ \ of\ packets\ \ received}{number\ \ of\ packets\ \ sent}$$

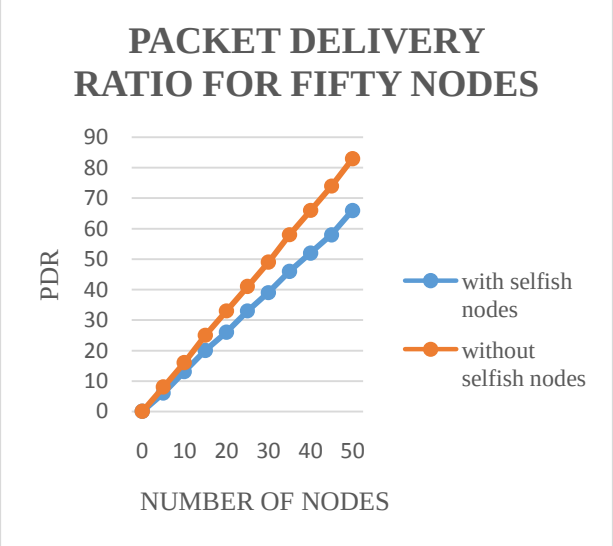

Fig-1 Packet delivery ratio with and without selfish node

The figure 1 depicts packet drop page with fifty normal nodes and one selfish node. The drop rate increases when there are selfish nodes in the network. So these types of nodes create problem in the network by dropping the packet or not forwarding packet to others.

The next comparison is performed with three selfish nodes among hundred normal nodes. The rate is increased due to the number of selfish node increment.

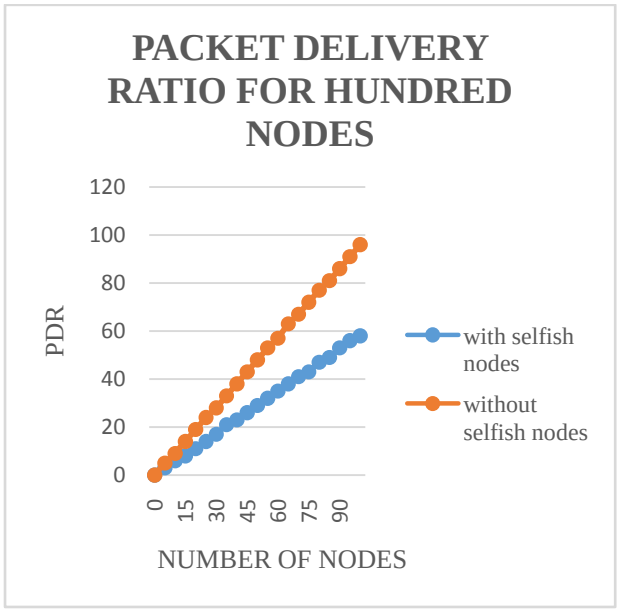

Fig-2 Packet delivery ratio with and without three selfish nodes

The figure 2 depicts the clear view of the packet delivery ratio with three misbehaving nodes. When it is compared with previous graph its impact is more because of increased amount of selfish node count by three. It has been shown that packet delivery is seriously affected in both cases of the network.

4.2.2. Delay:

It refers to the time taken for a packet to be transmitted across a network from source to destination. It also includes delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

$$\text{Delay} = \frac{\sum_i^n (CBR\ sent\ \ time - CBR\ received\ \ time)}{\sum_i^n CBR\ received\ \ time}$$

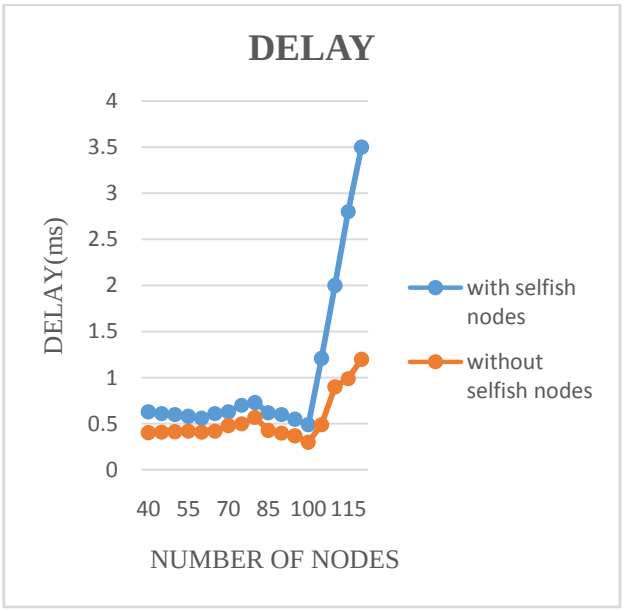

Fig-3 Delay with and without selfish nodes

The figure 3 is about delay caused in the network with and without selfish nodes. The delay increases drastically when there are selfish nodes so it is better to find and avoid it to make the data reach the destination.

5. CONCLUSION:

The work shows two types of results based on number of normal and selfish nodes. It is clearly shown in the graphical representation that there are so many changes in the network performance due to the misbehavior. When the count of the abnormal nodes is increased there is drastic drop in the packet which has been observed through packet delivery ratio. The delay is high when there are large numbers of selfish nodes. The impact of the selfish node is viewed in the MANET where it has increased the effect when abnormality is increased.

REFERENCES:

1. C. Toh, D. Kim, S. Oh, and H. Yoo, "The controversy of selfish nodes in ad hoc networks," in Proc. Adv. Commun. Technol., Feb. 2010, vol. 2, pp. 1087–1092.

2. C.K.N.Shailender Gupta andC.Singla,"Impact of selfish node concentration in MANETs," Int. J. Wireless Mobile Netw., vol.3,no. 2, pp. 29–37, Apr. 2011.

3. J.Hortelano,J.C.Ruiz,andP.Manzoni,"Evaluating the usefulness of watchdogs for intrusion detection in

VANETs," in Proc.Int.Conf. Commun. Workshop, 2010, pp. 1–5.

4. Enrique Hernandez-Orallo,Manuel David SerratOlmos,Juan-Carlos Cano,CarlosT.Calafate,andPietroManzoni,"CoCoWa:CollaborativeContanct-Based Watchdog for Detecting Selfish Nodes",IEEETrans.Mobile Computing.,June2015,vol. 14,pp. 1162-1175.

5. Bansal and M. Baker, "Observation-based cooperation enforce-ment in adhoc networks" arXiv:cs.NI/0307012,2003.

6. P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hocnetworks," in Proc. 6th Joint Working Conf. Commun. Multimedia Secur., 2002, pp. 107–121.

7. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems,"IEEECommun. Mag., vol. 43,no. 7, pp. 101–107,Jul.2005.