Misbehavior Routing Identification by Collaborative Contact Based Detection in MANET

Reshma.M[1],T.Manjula[2] and B.Anand[3]
PG Scholar[1],Assistant Professor[2],Associate Professor[3]
Hindusthan College of Engineering and Technology, Coimbatore, India
reshma.m33@gmail.com, *manjulavijaykumar83@gmail.com,* *b_anand_eee@yahoo.com*

Abstract - *The continuously self-configuring, Infrastructure less Mobile Ad-hoc Networks (MANETs) route in effective manner by utilizing the voluntary cooperating nodes. That is the ability of each node to move independently and freely, thus can configure the links to other nodes frequently. Certain node refuse to cooperate and leads to the selfish behavior and such nodes are named as selfish nodes, whose existence will degrade the network performance. A well-known existing method to detect such selfish nodes was the watchdog mechanism. Focusing only on this watchdog system alone will fail to detect all the selfish nodes, may generate false positives and negatives and thus by leads to wrong operation. Also it created poor system performance in terms of speed and precision. These were much important factors in the networks with sporadic contacts such as opportunistic and delay tolerant networks, because watchdog lack enough time and information to detect the selfish nodes. Thus propose a collaborative approach based on the diffusion of local selfish node awareness when a contact occurs. Thus the information about the selfish node is propagated quickly in the network, which leads to improved speed and precision while detecting the selfish nodes. With the help of other nodes can avoid such nodes while routing in the network.*

Keywords *– Cooperation, Delay tolerant networks, Mobile Ad-Hoc Networks (MANETs), Opportunistic Networks, Selfish nodes, Sporadic contacts.*

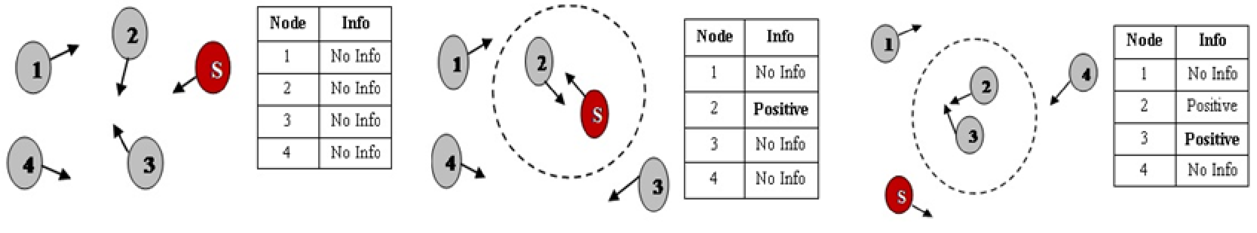
1 INTRODUCTION

Two categories of the cooperative networks which have great significance on now a day is the Mobile Ad-hoc Networks (MANETs) and Opportunistic and Delay Tolerant Networks (DTNs). The cooperation on these networks is usually contact based. Mobile nodes can directly communicate with each other if a contact occurs, if nodes are within communication range for a specific period of time. Supporting this cooperation is a cost intensive activity for mobile nodes. In the real world, nodes could have a selfish behaviour that is nodes being unwilling to forward packets for others [4]. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources, which may lead to network misbehaviour or the failure of the network operation and performance [3, 6]. There exist two main strategies to deal with selfish behaviour: a) motivation or incentive based approaches, and b) detection and exclusion. The first approach, tries to motivate nodes to actively participate in the forwarding activities. The detection and exclusion approach is a straight-forward way to cope with selfish nodes [5, 11]. In the collaborative contact based watch dog system we focus only on the detection of this selfishness. The node selfishness on MANETs has a huge impact on the overall performance of MANETs, such as the number of packets dropped, the offered throughput, and the probability of reachability reduces, Decreases the data accessibility and Increased delay time. In DTNs, selfish nodes can seriously degrade the performance of packet transmission; the packet may loss since selfish nodes do not provide the choice of retransmission [1, 8, and 13]. Detection of such selfish nodes very quickly and accurately is very essential for the overall performance of the network. One of the best existing methods to detect such selfish nodes is the watchdog mechanism. Watchdog systems operate in such a way that they have the capability to overhear wireless traffic and analyse it to decide whether neighbour nodes are behaving in a selfish manner or not [12]. When the watchdog detects a selfish node it is marked as a positive detection or if it is detected as a non selfish node it is marked as a negative detection. But when the watchdogs fail on this detection, they may generate false positives and false negatives that seriously degrade the behaviour of the system. Another problem is the presence of colluding or malicious nodes. In this case, the effect can even be more harmful, because such nodes try to disturb the correct behaviour of the network, such as one harmful malicious node can give wrong information about the status of other nodes, producing a fast diffusion of false negatives or false positives. The detection of such nodes is very much difficult to detect [7].

This paper introduces a new scheme called Collaborative Contact-based Watchdog for detecting selfish nodes, a method that combines local watchdog detections and the dissemination of this information on the network through contact among nodes. If a node has previously detected a selfish node it can transmit this information to other nodes when a contact new occurs. This way, other nodes have second hand information about the selfish nodes in the network. The goal of our approach is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives and the effect of malicious nodes also. The diffusion of information about positive or negative detections of selfish nodes introduces mainly two issues about the reputation of the neighbour nodes [2]. The first issue is the consolidation of information, that is, the trust about neighbour's positive and negative detections, especially when it does not match with the local watchdog detection and the second issue is the case of malicious nodes [9, 10]. In order to evaluate the efficiency of CoCoWa, an analytical performance model, that is modelling the network as a continuous time Markov chain (CTMC) and derives expressions for obtaining the time and overhead of detection of selfish nodes under the influence of false positives, false negatives and malicious nodes. There is a possibility of having a great reduction of the detection time of selfish nodes with a reduced overhead when comparing CoCoWa against a traditional watchdog. The impact of false negatives and false positives is also greatly reduced. Also the pernicious effect of malicious nodes can be reduced using the reputation detection scheme.

2 ARCHITECTURE AND OPERATION

If a node denies packet forwarding in order to save its own resources that is referred to as Selfish node. Because of this behaviour selfish node neither participates in routing nor relays data packets. A common technique to detect this selfish node is network monitoring using local watchdogs. A node's own local watchdog will overhear the packets transmitted and received by its neighbours in order to detect improper activities, such as the ratio between packets received to packets being retransmitted. By using this technique, the local watchdog can generate a positive or negative detection in case the node is acting selfishly or not respectively.



a) Initial State

b) Selfish contact (Positive), Local Watchdog Operation

c) Dissemination of information by Collaborative Contact

Figure.1 Collaborative contact based watchdog system operation. a) In the initial state the nodes do not have any information about the selfish node, the no info in the table. b) Node 2 detects the selfish node by using its own watchdog and marked as positive detection. c) Node 2 contacts with Node 3 and transmits the information about the selfish node in node 2 to the node 3. d) The local watchdog of node 4 fail to detect the selfish node and it generates a negative detection, actually a false negative. How a collaborative contact based watchdog works is outlined in the figure.1, with a consideration that there is only one selfish node. The figure shows that initially no node has information about the selfish node. When a node detects a selfish node using its own watchdog, it is marked as a positive, and if it is detected as a non selfish node, it is marked as a negative. When this node contacts another node, it can transmit this information to it; so, both nodes now store information about this positive (or negative) detection. Therefore, a node can become aware about selfish nodes directly by using its watchdog or indirectly, through the collaborative transmission of information that is provided by other nodes. The controlled diffusion of positive and negative detections is essential to prevent diffusion of wrong information. Figure. 2 show the functional structure of CoCoWa and which have three main components. The Local Watchdog has two functions: the detection of selfish nodes and the detection of new contacts. The local watchdog can generate PosEvt (positive event) when the watchdog detects a selfish node, NegEvt (negative event) when the watchdog detects that a node is not selfish, and NoDetEvt (no detection event) when the watchdog fails to detect information about the node, that is it does not have enough information about a node for detection. The detection of new contacts is such that when the watchdog overhears packets from a new node it is assumed to be a new contact, and so it generates an event to the network information module. The Diffusion module has two functions: the transmission as well as the reception of positive or negative detections. As the number of selfish nodes is low compared to the total number of nodes, positive detections can always be transmitted with a low overhead. But while transmitting only positive detections, false positives can be spread over the network very fastly. Thus, the transmission of negative detections is necessary to neutralise the effect of these false positives, but sending all known negative detections can be troublesome, producing excessive messaging or the fast diffusion of false negatives. Also, when the diffusion module receives a new contact event from the watchdog, it transmits a message including this information to the new neighbour node. When the neighbour node receives a message, it generates an event to the network information module with the list of these positive and negative detections.The Information Update module is for updating or consolidating the

information. A node can have the following internal information about other nodes: No detection state, Positive state and Negative state. A node can have direct information and indirect information, which is from local watchdog or through dissemination. CoCoWa is event driven, so the state of a node is updated when the PosEvt or NegEvt events are received from the local watchdog and diffusion modules. In particular, these events update a reputation value.

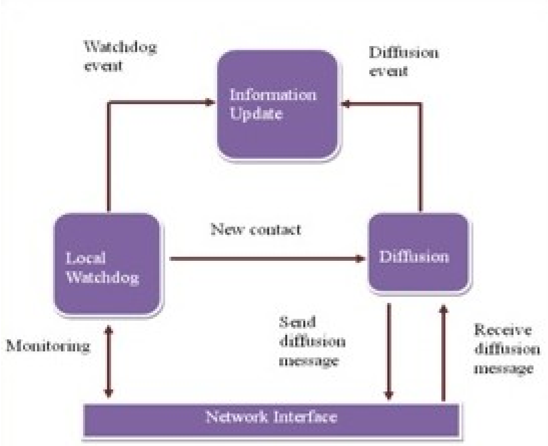


Figure.2. Collaborative contact based watchdog basic architecture

Behavior of malicious nodes is modeled from the receiver perspective, which is based on the probability of receiving wrong information about a given node when a contact with a malicious node occurs. This behavior is known as the maliciousness probability; aspects that can affect this probability are,

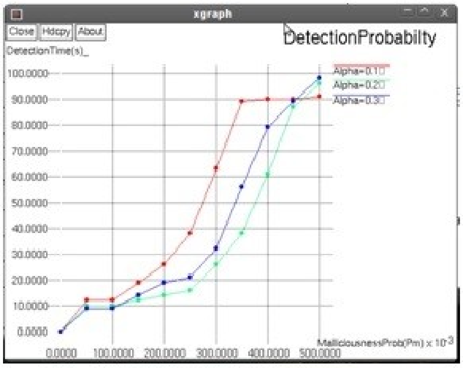
- The reception of information, considering that not all contacts produce this reception. An increase of communication range of the malicious nodes will increase the information reception.
- The malicious nodes do not have information about all nodes; so, in order to send a positive/negative about a node, they must have contacted this node previously or have received a message from other nodes.
- The proper generation of wrong information. From the receiver point of view, a perfect malicious node will always provide wrong information. In this case, the malicious node, in order to send wrong information, must know the state of each node. In other words it must have a perfect local watchdog, about the node it contacts.

3 ANALYTICAL EVALUATIONS

This section is devoted to evaluate the performance of CoCoWa. The analytical model has several parameters, so in this paper we focus on those parameters that clearly affect the performance.

3.1.1 DETECTION PROBABILITY

The probability of receiving wrong information about a given node when a contact with a malicious node occur on positive event and negative event /detection time depending on the number of nodes.



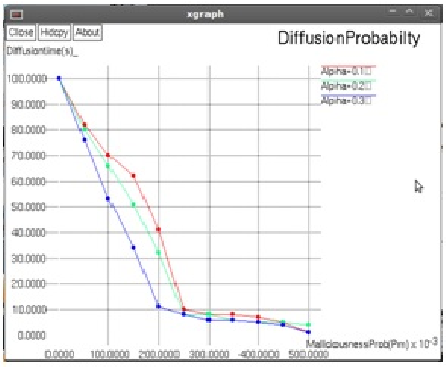


Figure 3.1. Detection Probability Vs Time.

Figure 3.2. Diffusion Probability vs time

Figure shows the malicious probability with respect to detection time on threshold value 0.1, 0.2, 0.3 increases depending on the ratio of false negatives. It evaluates the influence of collaboration for several values of Pc when only positive detections are transmitted. The detection time increases with the ratio of false negatives.

3.1.2 DIFFUSION PROBABILITY

It is the measure that gives the number of selfish nodes in the total number of nodes/total number of detections. The number of malicious nodes Pm depends on the number of nodes evaluated. If the ratio is low, the impact can be controlled using collaboration and reputation mechanisms, but if the ratio is high, the performance of the network can be very low. One malicious node for each ten collaborative nodes to the effect of selfish nodes, that only depends on the remaining cooperative nodes, and has less impact on network performance. These results are coherent, as they highlight the different behavior of selfish and malicious nodes with the threshold value 0.1, 0.2 and 0.3.

3.1.1 DETECTION TIME WITH DEGREE OF COLLABORATION

The global performance evaluation in the absence of false positives, false negatives and malicious node and only positive detections are transmitted. Taken in to consideration that there exists a sum total of N number of nodes, among which may have up to D=N-1 number of destination nodes. Also consider that the number of selfish nodes is one (S = 1), the simulation result gives the detection time for all nodes in a network and their dependence with different probabilities of detection (Pd). This probability of detection of selfish node is ranging from a low detection ratio (0.1), typical of DTNs and Opportunistic Networks, to greater detection ratios (0.3) typical of MANETs. When the degree of collaboration varies from 0 to 0.2, the detection time is getting reduced exponentially.

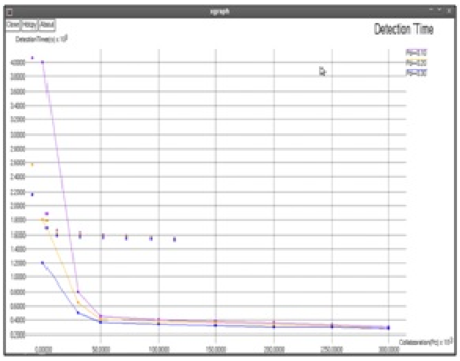


Figure3.3. Detection time vs Degree of Collaboration.

4 CONCLUSION

The CoCoWa as a collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the harmful effect of false positives, false negatives and malicious nodes. If malicious nodes spread false negatives or false positives in the network CoCoWa is able to reduce the effect of these malicious nodes quickly and effectively. Additionally, CoCoWa is also effective in opportunistic networks and DTNs, where contacts are sporadic and have short durations, and where the effectiveness of using only local watchdogs can be very limited. For the highly effective detection and collaboration of the selfishness we can implement multipath routing and multicast routing as a future enhancement.

REFERENCES

[1] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, “Impact of human mobility on opportunistic forwarding algorithms,” IEEE Trans. Mobile Comput., 2007.

[2] E. Hern_andez-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni, “Improving selfish node detection in MANETs using a collaborative watchdog,” IEEE Comm. Lett., vol. 16, no. 5, pp. 642–645, May 2012.

[3] H. Cai and D. Y. Eun, “Crossing over the bounded domain: From exponential to power-law intermeeting time in mobile ad hoc networks,” IEEE/ACM Trans. Netw., vol. 17, no. 5, pp. 1578–1591, Oct. 2009.

[4] J. Hortelano, J.-C. Cano, C. T. Calafate, M. de Leoni, P. Manzoni, and M. Mecella, “Black hole attacks in p2p mobile networks discovered through Bayesian filters,” in Proc. Int. Conf. Move Meaningful Internet Syst., 2010, pp. 543–552.

[5] K. Paul and D. Westhoff, “Context aware detection of selfish nodes in DSR based ad-hoc networks,” in Proc. IEEE Global Telecommun. Conf., 2002, pp. 178–182.

[6] L. Butty_an and J.-P. Hubaux, “Enforcing service availability in mobile ad-hoc WANs,” in Proc. 1st Annu. Workshop Mobile Ad Hoc Netw. Comput., 2000, pp. 87–96.

[7] L. Butty_an and J.-P. Hubaux, “Stimulating cooperation in selforganizing mobile ad hoc networks,” Mobile Netw. Appl., vol. 8, pp. 579 592, 2003.

[8] P. Hui, J. Crowcroft, and E. Yoneki, “Bubble rap: social-based forwarding in delay tolerant networks,” in Proc. 9th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2008, pp. 241–250.

[9] R. Groenevelt, P. Nain, and G. Koole, “The message delay in mobile ad hoc networks,” Perform. Eval., vol. 62, pp. 210–228.

[10] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, “Lightweight sybil attack detection in manets,” IEEE Syst. J., vol. 7, no. 2, pp. 236–248, 2013.

[11] S. Bansal and M. Baker, “Observation-based cooperation enforcement in ad hoc networks” arXiv:cs.NI/0307012, 2003.

[12] S. Buchegger and J.-Y. Le Boudee, “Self-policing mobile ad hoc networks by reputation systems,” IEEE Commun. Mag., vol. 43, no. 7, pp. 101–107, Jul. 2005.

[13] W. Gao, Q. Li, B. Zhao, and G. Cao, “Multicasting in delay tolerant networks: A social network perspective,” in Proc. 10th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2009, pp. 299–308. Oct. 2005.

AUTHORS PROFILE

Reshma.M obtained her B.E. in Electronics and Communication Engineering from CMS College of Engineering and Technology, Coimbatore (Anna University of Chennai, 2013) and pursuing M.E. in Applied Electronics from Hindusthan College of Engineering and Technology, Coimbatore (Anna University of Chennai). She is currently doing her project work on Mobile ad-hoc networks which includes security.

T.Manjula obtained her B.E. in Electrical and Electronics Engineering from Bharathiyar University, Coimbatore in 2004 and M.E. in Applied Electronics from PSG College of Technology, Coimbatore in the year of 2009. Currently she is working as an Assistant Professor in Hindusthan College of Engineering and Technology. Her area of interest is Wireless Communication and Embedded system.

Dr.B.Anand obtained his B.E degree from Government College of Engineering, Tirunelveli & M.E degree from Annamalai Univerity, Chidambaram. He completed his Ph.D. from Anna University, Chennai. He is currently working as an Associate Professor in Hindusthan College of Engineering and Technology, Coimbatore. His area of interest is Embedded system and Communication.