Improved collaborative watchdog system for detection of selfish node in MANET

Momin Kashif M[1], Prof. V. S. Kadam[2]
Department of Computer Engineering
Sinhgad Institute of Technology, Lonavala ,India

***Abstract*— A mobile ad hoc network (MANET) is a self-organized system comprised by multiple mobile wireless nodes. The node misbehavior due to selfish reasons can significantly diminish the performance of MANET. A selfish node attempts to use the resources only for its own purpose and it hesitates to share the resources with their neighbors. So, it is very important to detect the selfish nodes to improve the performance of MANET. Initially, an architectural model of a MANET is constructed and the communication between the mobile is originated. The packet drop can happen in MANET due to the selfish node or network congestion. In this paper, a distributed global trust is presented to improvise the detection of selfish node in the network in MANET. The main reason for using trust and reputation in this analysis is to accelerate the detection of misbehaving nodes. This study has been carried out in order to analyze the detection of selfish nodes on essential network functions such as routing and packet dropping. The simulation study demonstrate the proposed method enhances the selfish node detection ratio , packet delivery ratio(PDR), and average packet drop ratio.**

Index Terms- MANET, Selfish Node, Trust management, Reputation system.

I. INTRODUCTION

Cooperative networking is currently receiving significant attention as an emerging network design strategy for future mobile wireless networks. Successful cooperative networking can prompt the development of advanced wireless networks to cost-effectively provide services and applications in contexts such as vehicular ad-hoc networks (VANETs) or mobile social networks .Two of the basic technologies that are considered as the core for these type of networks are 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 (that is, if they are within communication range). Supporting this cooperation is a cost intensive activity for mobile nodes. Thus, in the real world, nodes could have a selfish behaviour, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources. The
impact of node selfishness on MANETs has been studied in [3]. In [2] it is shown that when no selfishness prevention mechanism is present, the packet delivery rates become seriously degraded, from a rate of 80% when the selfish node ratiois 0, to 30% when the selfish node ratio is 50%. The survey shows similar results: the number of packet losses is increased by 500% when the selfish node ratio increases from 0% to 40%. Therefore, detecting such nodes quickly and accurately is essential for the
overall performance of the network. Previous works have demonstrated that watchdogs are appropriate mechanisms to

detect misbehaving and selfish nodes. Essentially, watchdog systems overhear wireless traffic and analyse it to decide whether neighbour nodes are behaving in a selfish manner. When the watchdog detects a selfish node it is marked as a positive detection (or a negative detection, if it is detected as a non selfish node). Nevertheless, watchdogs can fail on this detection, generating false positives and false negatives that seriously degrade the behaviour of the system. Another source of problems for cooperative approaches is the presence of colluding or malicious nodes. In this case, the effect can even be more harmful, since these nodes try to intentionally disturb the correct behaviour of the network. For example, one harmful malicious node can be lying about the status of other nodes, producing a fast diffusion of false negatives or false positives. Malicious nodes are hard to detect using watchdogs, as they can intentionally participate in network communication with the only goal to hide their behaviour from the network. Thus, since we assume that these nodes may be present on the network, evaluating their influence becomes a very relevant matter. In this paper, a distributed trust is presented to improvise the detection of selfish node in the network in MANET. The main reason for using trust and reputation in this analysis is to accelerate the detection of misbehaving nodes. This study has been carried out in order to analyze the detection of selfish nodes on essential network functions such as routing and packet dropping. The simulation study demonstrate the proposed method enhances the selfish node detection ratio , packet delivery ratio(PDR), and average packet drop ratio.

II. ARCHITECTURE OVERVIEW

A selfish node usually denies packet forwarding in order to save its own resources. This behaviour implies that a selfish node neither participates in routing nor relays data packets. A common technique to detect this selfish behaviour is network monitoring using local watchdogs. A node's watchdog consists on overhearing the packets transmitted and received by its neighbours in order to detect anomalies, such as the ratio between packets received to packets being re-transmitted. By using this technique, the local watchdog can generate a positive (or negative) detection in case the node is acting selfishly (or not). An example of how

ISSN: 2278 – 7798

collaborative contact based watchdog works is outlined in figure 1. It is based on the combination of a local watchdog and the diffusion of information when contact between pairs of nodes occurs. A contact is defined as an opportunity of transmission between a pair of nodes (that is, two nodes have enough time to communicate between them). Assuming that there is only one selfish node, the figure shows how initially no node has information about the selfish node. When a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non selfish node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this information to it; so, from that moment on, both nodes store information about this positive (or negative) detections.

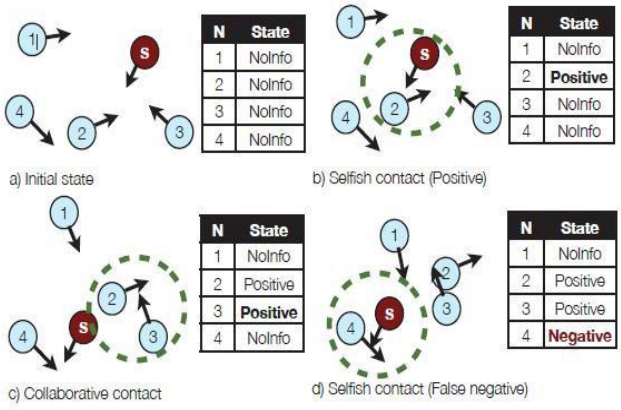


Fig. 1: *An example of how collaborative contact based watchdog works. a) Initially all nodes have no information about the selfish node. b) Node 2 detects the selfish node using its own watchdog. c) Node 2 contacts with node 3 and it transmits the positive about the selfish node. d) The local watchdog of Node 4 fails to detect the selfish node and it generates a negative detection (a false negative).*

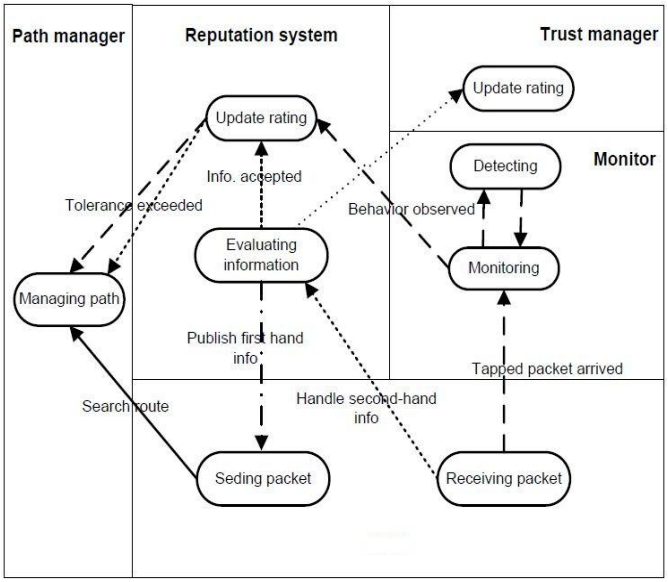


Fig2: Reputation system and trust Manger

In figure2 is enhanced work to the collaborative contact based watchdog system which detect the selfish node in the network by using watchdogs and second hand information , the second hand information is receive from the others node's watchdog . In above figure the Monitoring part is done by the watchdogs for detection node's selfishness behavior, if watchdog finds node is behave selfishness in the network then the Reputation system decreases the node's reputation, Trust manager is maintain the global trust of the node in the network which is used to improve the detection of selfish node in the network , if node's global trust is below the threshold value then Monitor easily detect the selfish node .

The dashed lines describe how the first hand information is collected. When a node *i* receives a packet from *j* ,then *i's* watchdog whether it is passive acknowledgment packet, if it is, the rating about *j* will be updated . If the reputation rating is greater than misbehaved threshold, it will inform Path manager to delete all the paths that contains the node *j* from the route cache of node *i*.

The dotted lines describe how second hand information published by the other nodes is handled. As seen in the figure, when node *i* receives published information it passes the information to the Reputation system to decide whether it should be accepted. If the information is accepted, the ratings about node *j* are updated. If the reputation rating after updating exceeds tolerance threshold, all the paths that containing the node *j* will be deleted from Path manager.

The dashed-dotted line describes that a node periodically publishes the reputation ratings it has about other nodes in the network. For reputation we are using Bayesian estimation.

A. Bayesian Estimation

Bayesian estimation is a statistical procedure which endeavors to estimate parameters of an underlying distribution based on the observed distribution [2]. Given a prior belief of the probability of some event happens, information that is acquired at each observation is update to reflect the added knowledge and to increase the precision of the belief. Equation 1 shows the Baye's theorem.

$$p(\theta_i|y) = \frac{p(y|\theta_i)P(\theta_i)}{\sum_{i=1}^{n} p(y|\theta_i)P(\theta_i)} \qquad \text{Equation-1}$$

Following example explains the meaning of the equation as well as illustrates how Bayesian analysis is used to predict the probability whether a node misbehaves or not. Suppose in the MANET a node *i* has never met node *j* before. *i* has a hypothetic prediction $P(\theta i)$ about the probability of whether node *j* will misbehave or not. Here θi is the ***model parameter*** representing a node misbehaves or behaves well. $P(\theta i)$ is the ***prior distribution*** which means a probability of θi before any data have been observed. After *I* has communicated with *j*, *i* gets observed data *y* about *j*. Then we can know $p(y|\theta i)$ a probability of the data *y* given a know parameter θi .

ISSN: 2278 – 7798

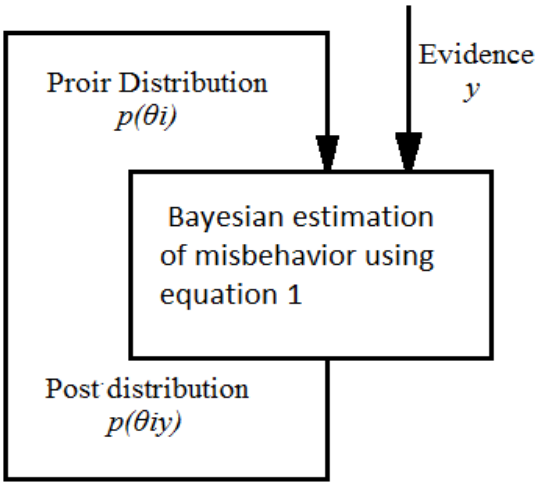


Fig3: Bayesian estimation of misbehavior

However, what we want to estimate is the probability of $i\theta$ given observed information y. It is called ***posterior distribution*** and expressed as $p(\theta i \mid y)$. With Equation 1, we can see that $p(\theta i \mid y)$ can be calculated if $P(\theta i)$ and $p(y \mid \theta i)$ are known. After $p(\theta i \mid y)$ is calculated, it will be used as the prior distribution in the next interaction. This approach of estimating a belief using Bayesian analysis is illustrated in Figure 3.

B. Proposed Algorithm

Step 1: Start

Step 2: Initialize two nodes as selfish nodes and two nodes as malicious nodes

Step 3: Find one hop neighbors for all nodes in network

Step 4: Initial Local watchdog system monitors node behavior

Step 5: Every Node will also receive indirect information about selfish nodes.

Step 6: Initially Local Watch dog system assigned NOINFO and this will be updated when a node finds a selfish node

Step 7: If a nodes finds its neighbor as selfish, then POSITIVE

Step 8: If a malicious nodes lie about selfishness then it will send NEGATIVE

Step 9: If a node found nothing then it will send NOINFO

Step 10: Indirect information is calculated

Node Reputation Calculation:

Node reputation = Local watchdog info + indirect info

Local watchdog info = +2 (if positive detection)

= -2 (if negative detection)

Indirect info = +1 (if positive detection)

= -1 (if negative detection)

= 0 (if Noinfo)

Step 11: Routing is done between source and destination, avoiding selfish nodes in routing path

III. SIMULATION RESULT

A. Simulation Environment

We performed our simulation using separate event network simulator ns2.34. Our network scenario consists of randomly placed 40 nodes within 2000 x 2000 m area. Simulation time was 720 seconds. Nodes were use 2- Mbps transmission rate with transmission range 250-m as we used IEEE 802.11 for MAC protocol. Data packet rate was 512bytes. We used AODV network layer multicast routing protocol with its default routing parameter values. We used one receiver with one sender and source sends packet with size 512 bytes. Attackers are randomly placed and randomly activated in order to imitate arbitrary nature of malicious node.

B. Performance Analysis

Following graph shows the packet loss, packet delivery ratio and end to end delay in the network.

Figure 4 shows the packet loss in the network. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent.

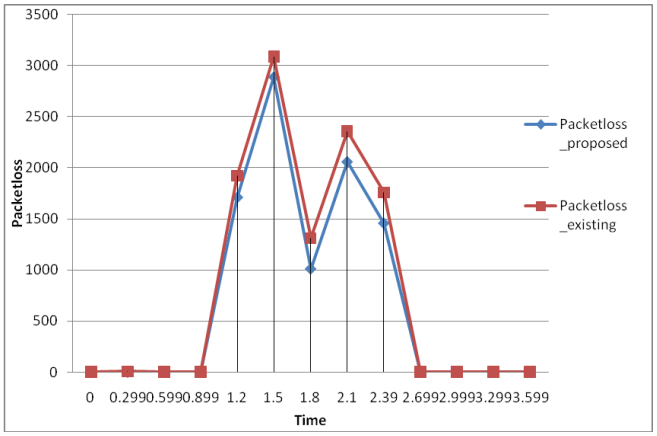


Fig4: Graph of packet loss

Figure 5 shows the packet delivery ratio (PDR) of project build to detect selfish node in the network

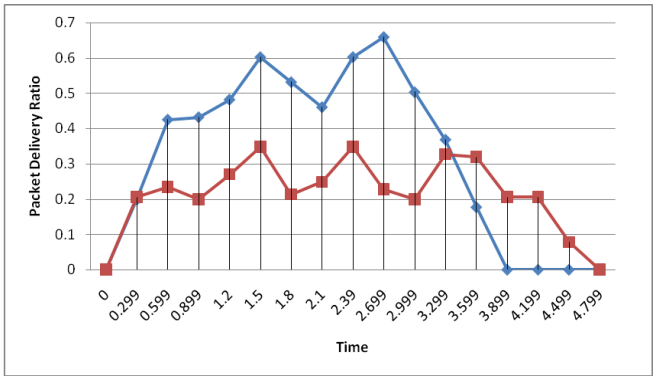


Fig5: Gragh of Packet Delivery Ratio

ISSN: 2278 – 7798

Figure 6 shows the end to end delay which is one-way delay refers to the time taken for a packet to be transmitted across a network from source to destination.

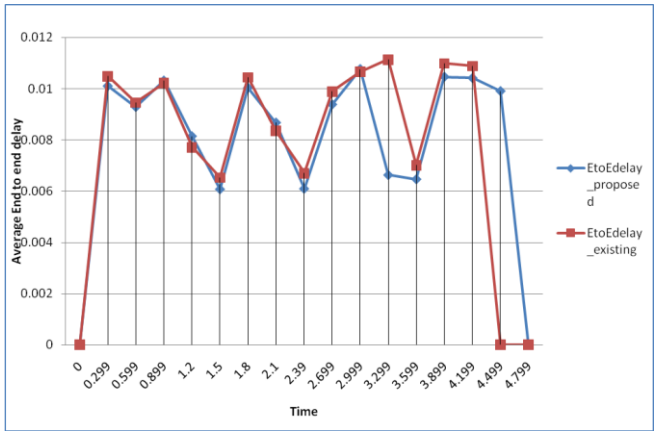
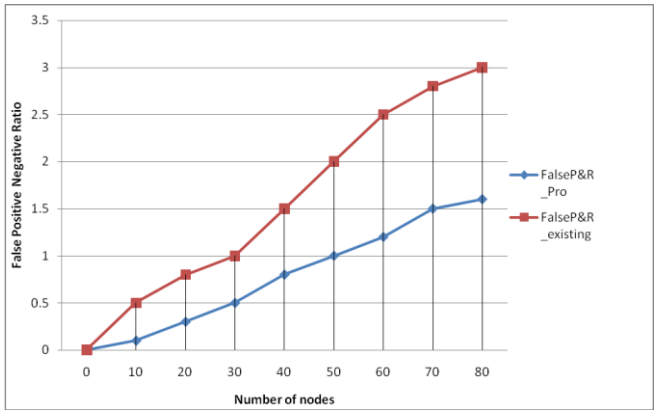


Fig6:Graph for End to End delay

Figure 7 shows the false positive and false negative ratio in the network.



IV. CONCLUSION

In this paper, an selfish node detection scheme is proposed that enables a routing protocol in MANETs to detect packet dropping attack by a malicious node. In the proposed mechanism, each node independently monitors the packet forwarding behavior of its neighbors. A cooperative mechanism is utilized among the nodes in the same neighborhood for detection of selfish or malicious nodes. The mechanism is simulated in network simulator and the results show that the scheme is highly robust, efficient and has improved performance mechanisms.

V. REFFERENCES

[1]Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni. A Collaborative Contact-based Watchdog for Detecting Selfish Nodes. IEEE Transactions on Mobile Computing, June 2014.

[2] J. Sengathir and R. Manoharan, “A futuristic trust coefficient-based semi-markov pre-diction model for mitigating selfish nodes in manets," EURASIP Journal on Wireless Communications and Networking, vol. 2015, no. 1, pp. 1-13, 2015.

[3] D. P. M. K. Reena Sahoo, “Detecting malicious nodes in manet based on a cooperative approach,” in IJCA Special Issue on 2nd National Conference- Computing, Communication and Sensor Network. CCSN, 2011.

[4] D. Djenouri and N. Badache, “On eliminating packet droppers in manet: A modular solution," Ad Hoc Networks, vol. 7, no. 6, pp. 1243-1258, 2009.

[5] S. Buchegger and J.-Y. Le Boudec, \Performance analysis of the con_dant protocol," in Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing, ser. MobiHoc '02. New York, NY, USA: ACM, 2002, pp.226-236.[Online].Available: http://doi.acm.org/10.1145/513800.513828

[6] D. Koshti and S. Kamoji, “Comparative study of techniques used for detection of selfish nodes in mobile ad hoc networks," International Journal of Soft Computing and Engineering (IJSCE) ISSN, pp. 2231{2307, 2011}.

[7] E. Hernandez-Orallo, M. D. S. Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, “A fast model for evaluating the detection of selfish nodes using a collaborative approach in manets," Wireless Personal Communications,Springer, vol. 74, no. 3, pp. 1099-1116, 2014.

[8] S. Gayathry and R. Gaur, “Handling sel_shness in manetsa survey," 2014.

[9] D.Anitha, Dr.M.Punithavalli.” A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS”. IJCSMC, Vol. 2, Issue. 3, March 2013, pg.112 – 119.

[10] Ramasamy Murugan, Arumugam Shanmugam.” A Timer Based Acknowledgement Scheme for Node Misbehavior Detection and Isolation in MANET”. International Journal of Network Security, Vol.15, No.4, PP.241-247, July 2013.

[11] M. D. Serrat-Olmos, E. Hern_andez-Orallo, J.-C. Cano, C. T. Calafate, and P. Manzoni. ”Collaborative watchdog to improve the detection speed of black holes in manets," 2012.

[12] Reshma Lill Mathew, Prof. P. Petchimuthu.” Detecting Selfish Nodes in MANETs Using Collaborative Watchdogs”.IJARCSSE, Volume 3, Issue 3, March 2013.

[13] The network simulator - ns2. http://www.isi.edu/ nsnam/ns/

ISSN: 2278 – 7798