I J C T A, 9(5), 2016, pp. 2265-2273
© International Science Press

A Collaborative Approach with Improved Performance byusing an Account-Aided Reputation Management System in MANETs

Kaviarasi K.* and Ranjani S.**

ABSTRACT

The co-operation in MANETs is a cost-intensive activity and some nodes can pass up to cooperate, leading to a selfish node behaviour. Thus, the long range affirm could be solemnly affected. The use of watchdogs is a reputable mechanism to detect selfish nodes. However, the detection technique performed by watchdogs can fail, give rise to false positives and false negatives that can persuade to wrong operations. This is distinctively important on networks where sometimes watchdogs lack of enough time or information to detect selfish node. A way to reduce the detection time and to improve the accuracy of watchdog mechanism is the collaborative approach. Collaborative Watchdogs mechanism is based on the diffusion of local selfish nodes aliveness when a contact occurs, so that tidings about selfish nodes is quickly propagated. This approach reduces detection time and increases the preciseness when detecting selfish nodes and to reduce number of selfish node in a network using account management and reputation management can be done further. ARM integrates reputation and price systems by enabling highly reputed nodes to pay less for their received services.These proposed mechanism have perform well on data transportation time, data retrieval time and messages cost against existing approaches.

Keywords: Selfish Nodes, Watchdog Mechanism, Collaborative Approach, False Positives, False Negatives, Reputation Management and account Management.

1. INTRODUCTION

In a MANET, nodes can purposely move around while communicating with each other. These networks may underperform in the presence of nodes with a selfish behavior, expressly when operating under energy constraints. A selfish node habitually will not cooperate in the transmission of packets, seriously affecting network performance [1][3]. Although less frequent, nodes may also fail to cooperate either designedly or due to faulty software or hardware. Watchdog mechanism is used to detect the selfish nodes. once the selfish node is detected, then it is marked as a positive detection (or a negative detection, if it is detected as a non selfish node). However at the slammer time, watchdog mechanism can also fail on this detection, accomplish false positives and false negatives that seriously vitiate the behaviour of the system. So the collaborative contact-based watchdog mechanism is used as a new scheme for detecting selfish nodes that combines local watchdog detections and the promulgation of this information on the network. If one node has previously detected a selfish node it can transmit this information to neighbour nodes when a connection occurs. This collaborative approach is helpful to reduce the detection time and to improve the preciseness by reducing the backwash of false positives and false negatives.

2. SYSTEMMODEL

The performance is based on the combination of a local watchdog mechanism and the diffusion of information when contacts between the nodes occurs. A contact is defined as a good fortune of transmission between a pair of nodes.

Figure1: Modules in collaborative approach &their connections

The diagram shows the architecture of the collaborative approach model which reveals the way to find out the selfish nodes. The Local Watchdog module has two functions: the detection of selfish nodes and the detection of distinct contacts. The local watchdog can bring to pass the following events about neighbour nodes: (positive event) when the watchdog detects a selfish node, (negative event) when the watchdog detects that a node is non selfish, and (no info event) when the watchdog does not have bounteous information.

The EVENT update module is driven by the previous local and indirect events. These events update the reputation about a node, and are used to finally decide if a node is selfish or not using the threshold. The Diffusion module has two functions: the transmission as well as the accession of positive (and negative) detections. A pivotal issue to approach is the diffusion of information. As the number of selfish nodes is low-hanging while compared to the total number of nodes, positive detections can repeatedly be transmitted with a low wiretap. Updating or consolidating the information is another key issue. This is the function of the Information Update module.

PosEvt event: the node commerce with the selfish node and the watchdog detects it, with probability p_d(1"pf_n). Note that a false positive can bring to pass with probability $p_d \cdot pf_p$.

NegEvt event: the node contacts with a non-selfish node and detect it with probability $p_d(1–pf_p)$. A false negative can also be generated when it contacts with the selfish node with probability $p_d \cdot pf_n$.

The formula can be written as, $\rho = \rho + \Delta$.

The values of Δ can be differ according to the performance of the nodes. where $\Delta = + \delta$(PosEvt, Local), + 1(PosEvt), –δ (NegEvt, Local), –1(NegEvt, Indirect).

The information update module is driven by the previous local and indirect events. These events update the reputation about a node ñ, and are used to finally decide if a node is selfish or not using the threshold θ.

Here, analytical model for evaluating the performance of collaborative approach can be done. The goal is to obtain the detection time (and overhead) of selfish node in a network. This model takes into account the backwash of false negatives. False positives do not upset the detection time of the selfish node, so pf_p is not fixed up in this model. Using λ as the contact rate between nodes, we can model the network using a 4D Continuous Time Markov chain (4DCTMC). For modelling purposes, the collaborative nodes are divided into two sets: a set with D destination nodes, and a set of E = C – D intermediate nodes. The destination and intermediate nodes have the same behaviour (both are collaborative nodes). The only aspiration of this division is to provisionally obtain the time and the overhead required for the subset of destination nodes to detect the selfish node. The network is sculpt as a set of N mobile nodes, with C collaborative nodes, M malicious nodes and S selfish nodes (N = C + M + S). Here, main intention is to grab the time and overhead that a firm of D≤C nodes are must to detect the selfish nodes in the network. The overhead is the number of

information messages dispatched up to the detection time. The effect of having several selfish nodes in a network is easy to evaluate, and it does not require a specific model. If we assume that selfish nodes are not cooperative, we can analyses the impact of each selfish node on the network independently. In the case of several selfish nodes (S > 1) on a network with N nodes, we can assume that there are C = (N – S) cooperative nodes.

3. NODE CONTACTS

3.1. Selfish Contacts

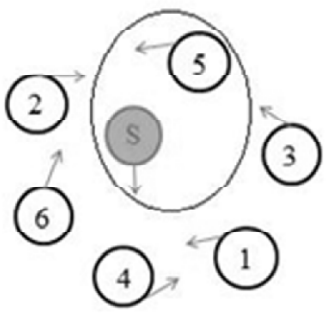
Let us consider, One of the nodes is the selfish node. Then, the collaborative node *can* detect this selfish node using its watchdog and have a positive about this selfish node. Inspite of that, a contact does not always insinuate a detection. Here, probability of detection (p_d) is introduced to render the model. This probability depends on the effectiveness of the watchdog (for example if the contact time is less, the watchdog does not have enough information to appraise if the node is selfish or not). In this fig, the selfish node S can be identified by the neighbour node 5 by its own watchdog mechanism.

3.2. Collaborative Contact

Both nodes are collaborative. In this case, if one of them has one or more positives, it can transmit this information to the other node. So, from that occasion, both nodes have these positives. As in the selfish contact case, a contact does not always imply a collaboration. This model can be designed with the probability of collaboration (p_c). The degree of collaboration is a unbounded parameter of the network to be evaluated. This value is used to reflect that either a message with the intimation about the selfish nodes is lost or that a node temporally does not collaborate. In real networks, full collaboration ($p_c = 1$) is always impossible. In the fig 3, the information about the selfish node S is diffused by the node 3 to node 5, this shows the collaborative approach.

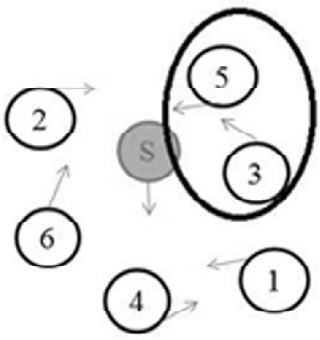
4. GLOBAL PERFORMANCE EVALUATION

The number of selfish nodes is one (S = 1) and the detection parameters are: $\theta = \delta = 1$. Here observe shows that, when increasing the degree of collaboration from 0 to 0.3, the detection time is reduced exponentially and the overhead is increased. The effect of p_d is expected: for pre-eminent values of p_d, the detection time is reduced. Thus, even for a low collaboration rate, the detection time for all nodes is abridged with an overhead with respect to the messages, which represents an improvement of detection time. So Collaborative approach is useful in both Opportunistic Networks and DTNs. When using the local watchdog alone, the detection time is very high (close to one hour). The implications are important. One hour detection is not useful, because it is equivalent to no detection. Thus, when using collaboration, the detection time is reduced from hours to seconds, meaning that nodes can take appropriate actions in time to avoid the selfish nodes, thereby improving the



N	STATE
1	No Info
2	No Info
3	No Info
4	No Info
5	Positive
6	No Info

Figure 2: Selfish Contact



N	STATE
1	No Info
2	No Info
3	positive
4	No Info
5	positive
6	No Info

Figure 3: Collaborative Contact

network performance. For the experiment, the values can be set as $p_d = p_c = 0.2$. A value of D = N –1 evaluates the detection for all collaborative nodes in the network (the overall detection), and D = 1 evaluates the detection time for only one node (the individual detection). Thus, the overall detection evaluates the performance of the outright network, while the individual detection evaluates the performance seen from an arbitrary node. We observe that, in general, the greater the number of nodes, the smaller the detection time and the higher the number of messages. The prevailing reason is that, when the number of nodes is greater, the number of contacts increases and so the information about the positive detection is promulgated more fleetly [2]. The cost is directly proportional to N. Now, Evaluation of the detection function, that is the impact of the è and ä parameters. Here, expectation is that greater è values imply greater detection times and overhead, due to the number of events required to make a decision. In the plot we can also observe that increasing ä, that is, giving more trust to local events, implies a reduction of both detection time and overhead. The significance of these detection parameters will become more evident when handling malicious nodes. Finally, the effect of having several selfish nodes S >1 is easy to evaluate. Since the number of cooperative nodes is reduced when S increases (C = N " S), the effect is similar to reducing the number of nodes in the network. For example, a network with N = 100 and S = 5 has a behaviour similar to a network with N = 96 and S = 1. Thus, the harmful effect of selfish nodes depends mainly on the number of remaining collaborative nodes.

5. ANALYTICAL EVALUATION AND RESULTS

These analysis helps to determine the transmission of packets by other nodes when the selfish node is present over the network and the effects of false positives and false negatives over other normal nodes.

5.1. Evaluation of Detection Time Dependingon Numberof Nodes

The fig. 4 shows the relationship between the number of nodes and the detection time, where the probability of the detection time $P_d = P_c = 0.2$. The value of N ranges from 1 to 50. A value of D = N – 1 evaluates the detection for all collaborative nodes in the network (overall detection) and D = 1 figure out the detection

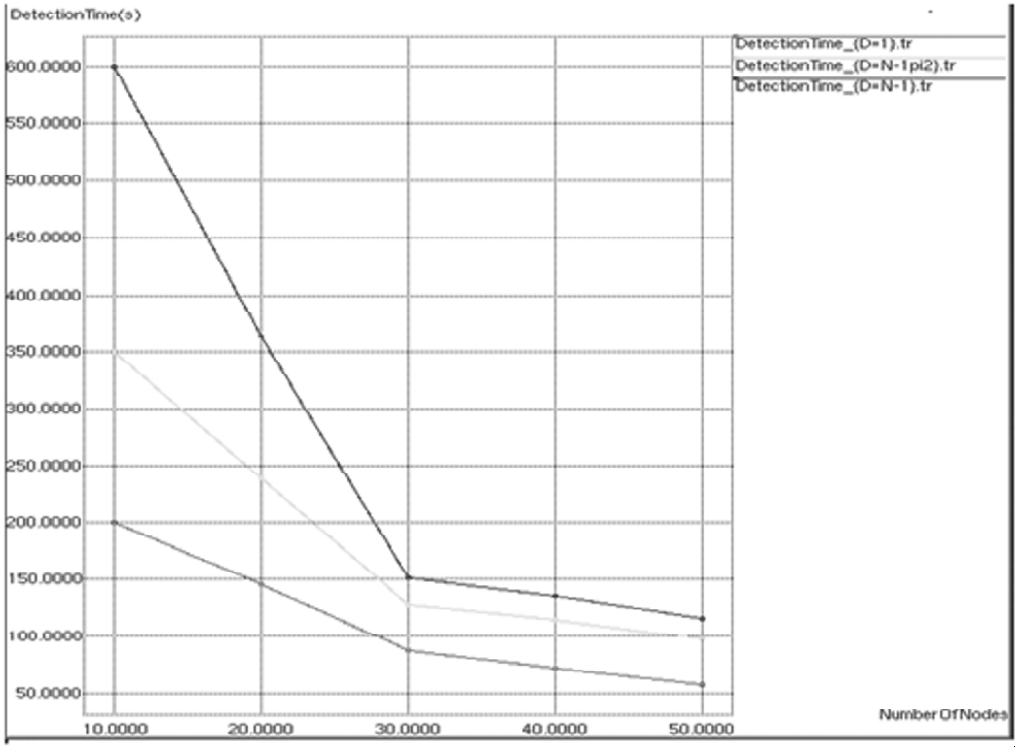


Figure 4: No. of Nodes Vs Detection Time

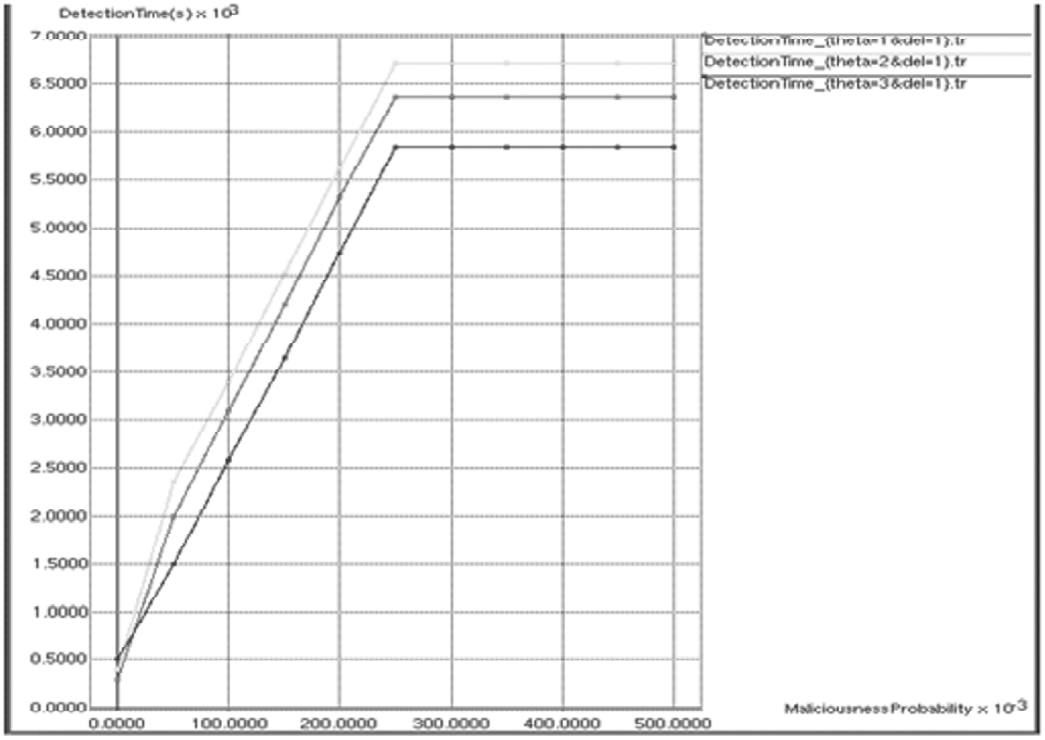


Figure 5: Effects of Malicious Nodes

time for only one node. Thus the overall detection evaluates the performance of the entire network. In general the greater the number of nodes, smaller the detection time and greater the number of messages. The foremost reason is that, when the number of node increases, the number of contacts increases and so the information about the positive detection is promulgated more quickly.

5.2. Strikeof Malicious Nodes

Here, the effect of malicious nodes can be figured out. Fig. 5 shows the detection time of a selfish node depending on the maliciousness probability of one node (M = 1). This ratio range from 0 (no malicious behaviour) to 0.5 (a very malicious behaviour). The parameters used are similar to N = 50, D = 1, $pf_n = p_d$= 0.1, $\theta = \delta = 1$, $\gamma = 0.1$. Here conclusion says that when p_m increases the detection time increases. This effect is reduced for greater degrees of collaboration. Nevertheless, for values of $p_m < 0.3$, the impact is very reduced, meaning that collaboration reduces the impact of malicious nodes. It also shows that the diffusion time is reduced when p_m increases. Increasing the degree of collaboration reduces this diffusion for low values of p_m [6]. Thus the collaboration cannot reduce the impact of malicious nodes for $p_m > 0.2$. Therefore, in order to reduce this impact, the adjustment of the values of the detection parameters is needed. In this case, more trust can be given to the local watchdog [5]. This is confirmed by the results, using $p_c = 0.2$. The best results are obtained for $\delta = \theta = 2$ and $\delta = \theta = 3$. Although the detection time is greater compared to $\delta = \theta = 1$for low values of p_m, when p_m is high, the detection time does not increase exponentially as for p_m = 1. Greater values of δ and θ (not shown in the graph), increases the detection time. Thus, given too much trust to the local watchdog is away to elude collaboration, so the detection time is increased. If the ratio M/ N is low, the impact can be controlled using collaboration and reputation mechanisms, but if the ratio M/N is high, the performance of the network can be very low.

6. METHODOLOGY TO OVERCOME COLLABORATIVE APPROACH

The effect of selfish nodes can be handle by giving credits to the cooperative nodes rather than the selfish nodes. Thus the packet transmission can also be done by faster way and efficiency of the node can also be improved.This can be applicable by the reputation management, account management methods.

6.1. Reputation Management

The Reputation administrator in reputation management collects the reputation information from all the nodes in its region to globally compute the reputation and maintain the account for mobile nodes. The reputation and account management uses this global reputation value to detect the misbehaving nodes in the Network. As the global information is used to calculate the reputation value instead of using local information, the SRA can provide accurate reputation values [7]. The use of global information enables the R&A management system to detect the wrong reputation values and misreported information. In Reputation and Account Management, the watchdog mechanism is used to listen the packet forwarding behaviour of nodes. The node which continuously observes the forwarding behaviour of the neighbour nodes is called as observer. The observer save two values using watchdog such as the number of packets received by node for forwarding and the number of packets has forwarded by the node during time duration T. The observer node n_o computes the reputation value of node n_i using the equation.

$$R_i^{no} = D_i^r / D_i^f$$

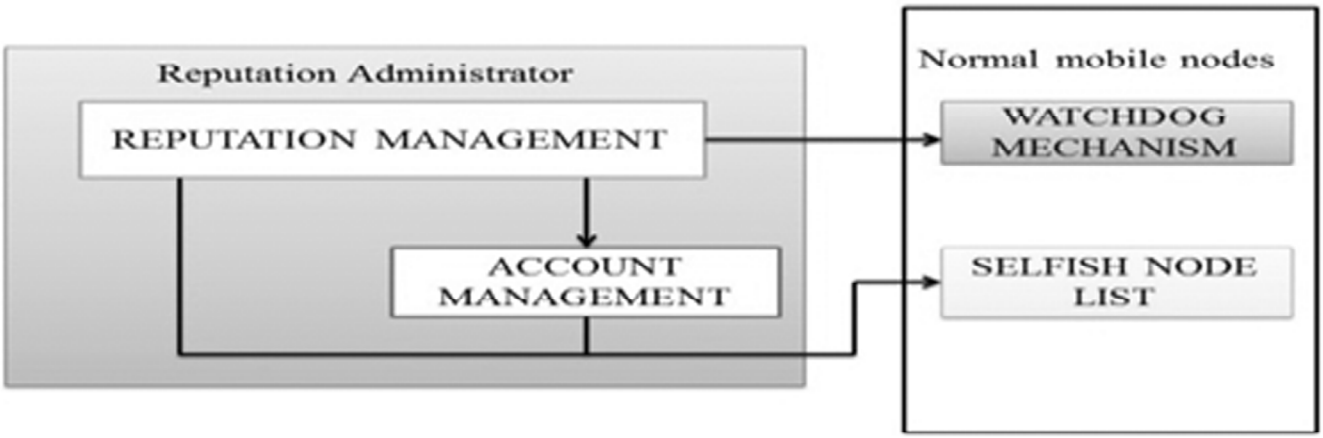


Figure 6: Block Diagram of Account &Reputation Management

6.2. Account Management

Account Management system maintains the account for each node to ignore the equal treatment of highly reputed nodes in the different reputation levels. This will induce the cooperation maintains the account for each node comes under its transmission range and increase or decreases the credit values from the account for their forwarding services or receiving services. The credit values need not to be circulated in the network in SRA like existing price system. This system calculates the credit earned by the nodes by using the value of percentage of number of packets forwarded with respect to number of packets received for forwarding. The credit is computed by the equation, $P_e = P_r R^i_g$. The constant credit rewarding factor is denoted by P_r and the percentage in SRA of node n_i is R^i_g. The administrator increases the credit in the account of nodes in its region by p_e. This will encourage the nodes to participate in communication without selfishness.

7. RESULTS AND DISCUSSION

In this method, The maximum reputation value is calculated from 0 to 1. Thus the threshold value can be calculated as 0.2. Here the account details can be maintained bysingle node. That single node can maintain the accounts of all other neighbourhood nodes. This node is named as admin node. Finally the table can be created, which consists of identity number of a node and the reputation value of corresponding nodes and the account number of nodes. Thus the detection time of theselfish node can be decreased while comparing the normal collaborative approach. This is due to increase in the credits of a normal nodes which transmitting the information to the other nodes.

7.1. Decrease in the number of Selfish Nodes

The detection time increases eventually when the reputed nodes takes place in the transmission. Thus the reputation management system approach shows that the efficiency of the node can be increased and thus it leads to increase in the throughput. Thus the graph shows that the selfish nodes reduced when the reputed and the account values are considered for the nodes while transmitting packets.

7.2. Decrease in the rate of False positive and False Negative

The following graphs shows the reduction in the False positives and False Negatives. In case of reputation and account Management, the credits can be earned by the nodes which sending more packets. By considering this, all other un co-operative nodes can be avoided.

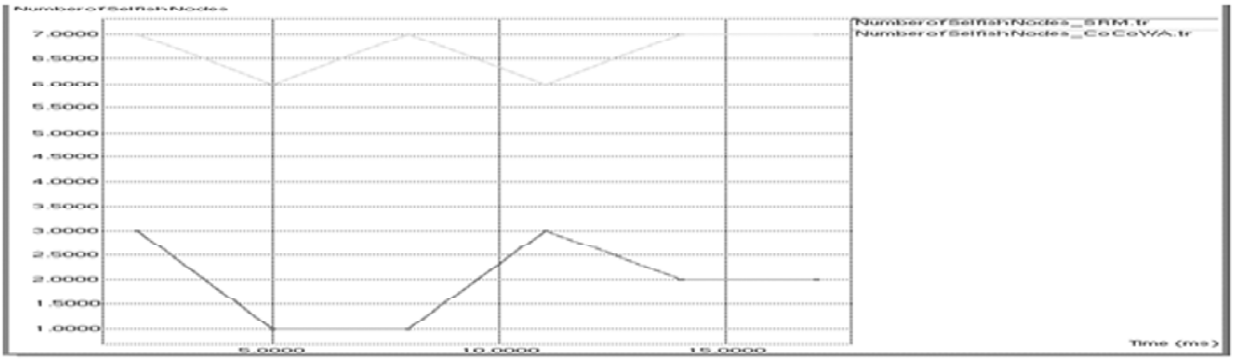


Figure 7: Reduction of Selfish Nodes

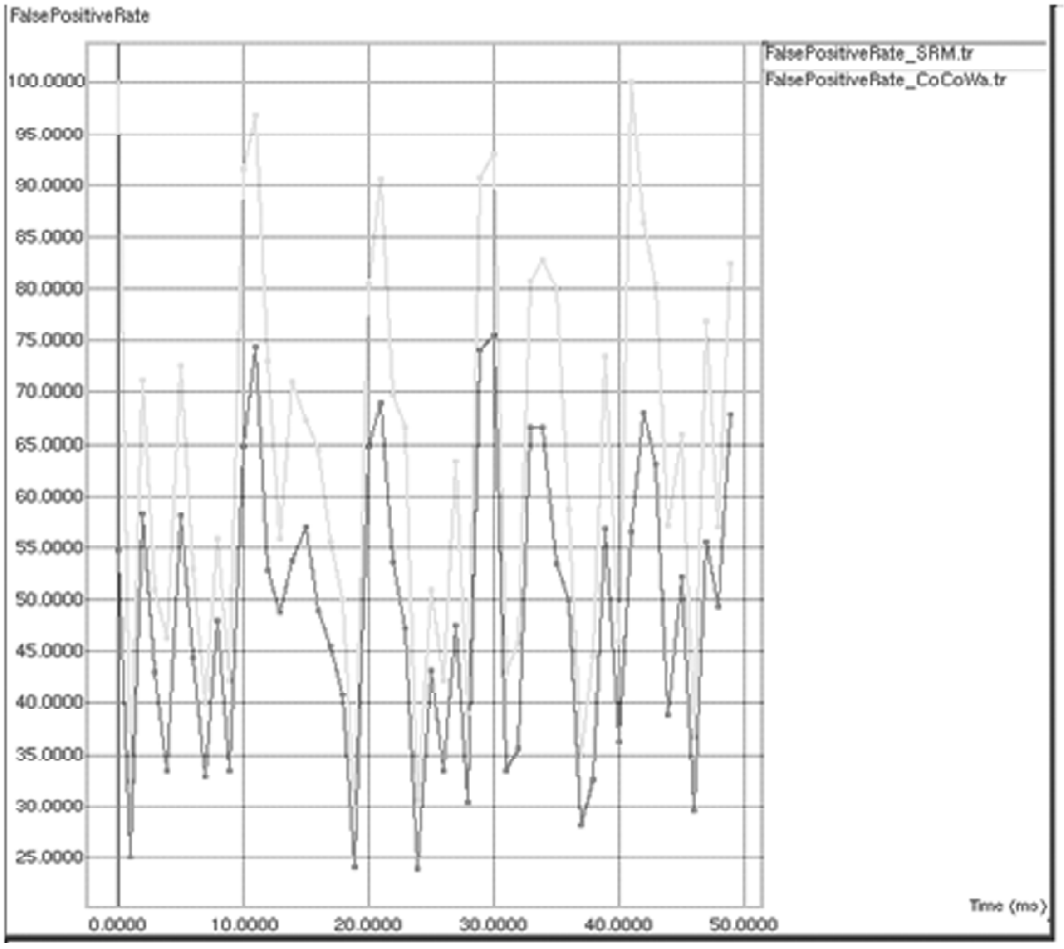


Figure 8: Reduction in False Positives

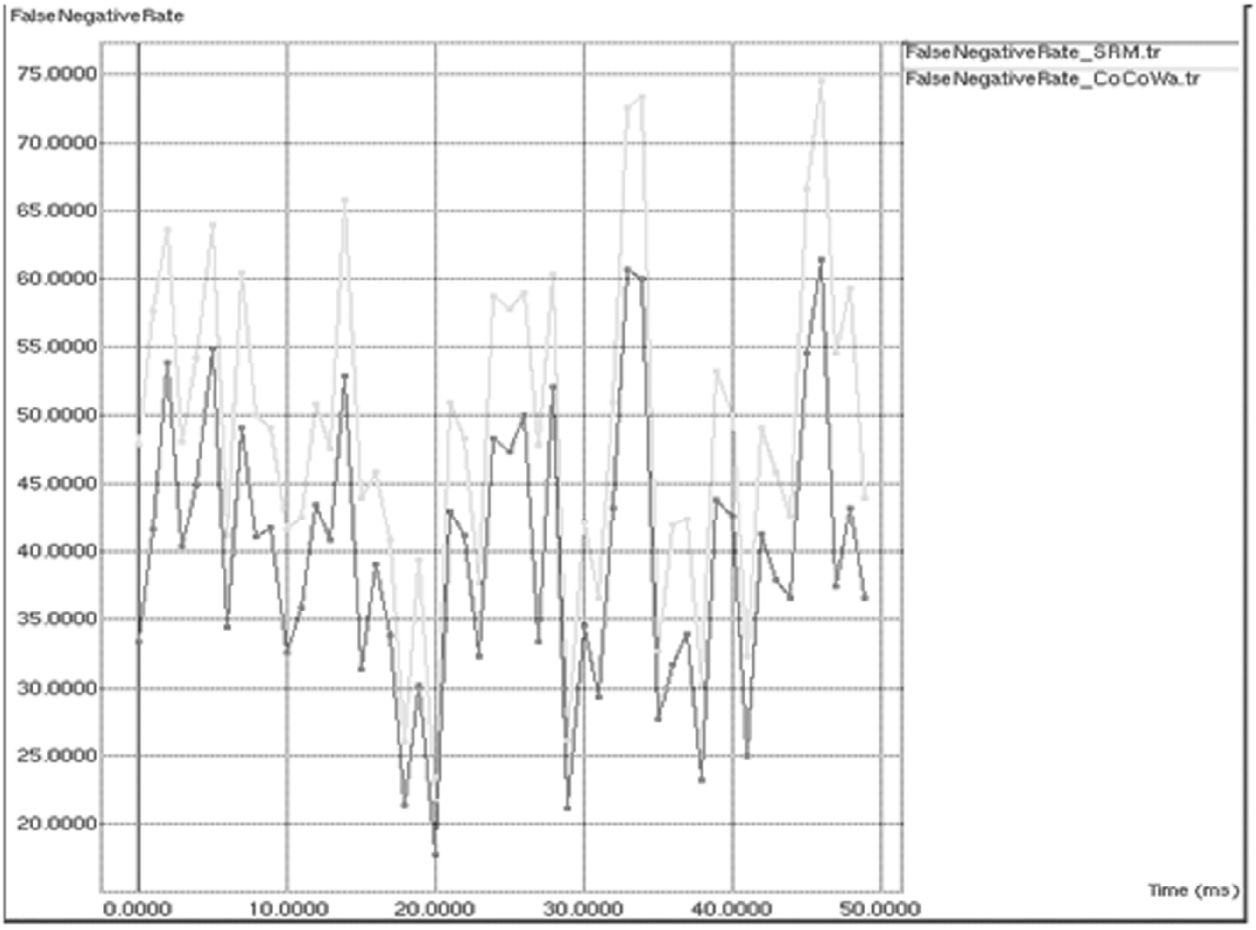


Figure 9: Reduction in False Negatives

The reduction in the selfish nodes leads to the efficient packet transmission and thus the watchdog mechanism can also be active while sending information about the selfish node as the number of selfish node is decreased. It automatically leads to the reduction in the number of False Positives and False Negatives.

8. CONCLUSION

Account and Reputation Management system is to efficiently and effectively detect selfish node behaviors and provide cooperation incentives.Reputation Management intelligently combines a reputation system and a price system. It builds upon an underlying locality-aware Distribution Hash Table infrastructure to efficiently collect global reputation information in the entire system for node reputation evaluation, which avoids periodical message exchanges, reduces information redundancy, and more accurately reflects a node's trust. Account and Reputation Management has functions for reputation management and account management, the integration of which fosters cooperation incentives and unco-operation deterrence. This approach can detect uncooperative nodes and increase the efficiency of the networks by decreasing the effects of False Positives and False Negatives. Thus the packet transmission can be improved finally.

REFERENCES

[1] Agrawal, M. and Datar, P. *"Finding selfish nodes in mobile adhoc network"*. ISSN-2(2014).

[2] E.H. Orallo, M.D. Serrat Olmos, J.C. Cano and P. Manzoni. *"Evaluation of collaborative selfish node detection in manets and dtns"*. ACM MSWiM, New York, (2012).

[3] Gupta, C. S. and Singala.C. *"Impact of selfish node concentration in manets."* IJWMN, 2, 29-37, (Apr 2011).

[4] C. Toh, D. Kim, S. O. and H. YOO. *"Controversy of selfish nodes in ad-hoc networks"*. ICACT, 2, 1087–1092, (2010).

[5] F. Karl, A. Klenk, S. Schlott, and M. Weber. "*Advanced detection of selfish or malicious nodes in ad-hoc network*". ESAS, 152-165, (2004).

[6] M. Hollick, J. Schmitt and Steinmetz. R. "*On the effect of node misbehavior in ad-hoc networks*". Vol. 499, ICC, 3759-3763(2014).

[7] R. Akbani, T. Korkmaz, and G. V. Raju, "*Emltrust: An enhanced machine elearning based reputation system for manets*," Ad Hoc Netw., vol. 10, no. 3, pp. 435-457, (2012).