INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 12 ISSUE 1 – APRIL 2016 - ISSN: 2349 - 9303

Detecting the MAC Selfish Node Using Collaborative Contact Based Watchdog Method (COCOWA)

C.Poornima
II year M.E. Applied Electronics, Akshaya College of Engineering and Technology, Coimbatore
c.poorni777@gmail.com

Mr. S.Gladwin Moses Stephen
Asst. Prof. ECE Dept., Akshaya Colleg of Engineering and Technology, Coimbatore
gladwinmoses@gmail.com

Abstract- In Mobile ad-hoc networks (MANETs) assume that mobile nodes voluntary cooperate in order to work properly. This cooperation based cost-intensive activity and some nodes refuse to cooperate, leading to selfish node behavior. The overall network performance will be seriously affected. Thus use of watchdogs is a well-known mechanism to detect selfish nodes. Therefore the detection process performed by the watchdogs can fail, generating false positives and false negatives that leads to wrong operations. Moreover, relying on the local watchdogs alone can lead to a poor performance when detecting selfish nodes, in provisions of speed and accuracy. In ad hoc network, the selfish nodes deviating from the standard MAC (Medium Access Control) protocol can significantly degrade the normal nodes' performance and it is difficult to detect. In this paper, we propose the detection and defense schemes to identify and protect against MAC-layer selfish misbehavior, respectively, in IEEE 802.11 multi-hop ad hoc networks.
Index Terms –IEEE 802.11, COCOWA Method, Content based Watchdog method

1. INTRODUCTION

Wireless Sensor Network (WSN) are a trend of the past few years, and they involve deploying a large number of small nodes. The nodes then sense environmentalChanges and report them to other nodes over flexible network architecture.Cooperative networking is currently receiving thesignificant attention as adeveloping network design strategy for the 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 networks. Two of the basic technologies that are considered as the core for these types 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 behavior, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources. The literature provides two main strategies to dealwith selfish behavior: 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. Therefore, detecting such nodes quickly and accurately is essential for the overall performance of the network. PreviousWorks have demonstrated that watchdogs are appropriate mechanisms to detect misbehaving and selfish nodes.

Essentially, watchdog systems overhear wireless traffic and analyze it to decide whether neighbor nodes are behavingIn a selfish manner [16]. When the watchdog detects a selfish node it is marked as a positive detection (or a negativeDetection, 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 behavior of the system.

Communication protocols are usually designed under the assumption that all participants would comply with the

regulations. However, in untrusted communication environments, a misbehaving user can deviate from the regulations and cause damage to or obtain performance gain over other honest parties. Thus, trustworthy communication is a crucial issue, especially in wireless ad hoc networks where nodes need to fully cooperate with each other to ensure correct route establishment, successful packet delivery, and efficient resource usage. Traditional approaches to providing network security are mostly cryptography based. Unfortunately, they cannot be used to address user misbehavior at the Medium Access Control (MAC) layer.MAC layer misbehavior can be generally classified into the following two categories: malicious misbehavior and selfish misbehavior One kind of malicious misbehavior is jamming attack [1], [8], which is one particular type of Denial-of-Service(DoS) attack [2], [9], [10]. The malicious users could either constantly generate strong signals to overwhelm normal nodes' signals, or transmit fake packets to occupy the shared channel or hence prevent the normal users from communicating.

This paper introduces Collaborative Contact-based Watchdog (Cocowa) as a new scheme for detecting selfishNodes that combines local watchdog detections and the dissemination of this information on the network. IfOne node has previously detected a selfish node it can transmit this information to other nodes when a contactOccurs. This way, 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 negativesand false positives. Although some of the aforementioned papers (such as [3], [28]) introduced some degree of collaboration on their watchdog schemes, the diffusion is very costly since they are based on periodic messageDissemination. The diffusion of information about positive or negative detections of selfish nodes introduces several issues about the reputation of the neighbor nodes. The first issue is the consolidation of information, that is, the trust about neighbor's positive and negative detections, especially when it does not match with the local watchdog detection. Another issue is the case of malicious nodes. Thus, this paper extends our previous approaches [12], [13] to also cope with malicious nodes using a reputation scheme. In order to evaluate the efficiency of Cocowa we first introduce an analytical performance model. We model the network as a continuous time Markov chain (CTMC) and derive expressions for obtaining the time and overhead (cost) of detection of selfish nodes under the influence of false positives, false negatives and malicious nodes. In general, the analytical evaluation shows a significant 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. Finally, the pernicious effect of malicious nodes can be reduced using the reputation detection scheme. We also evaluate Cocowa with real mobility scenarios using well known human and vehicular mobility traces. These experimental results confirm that our approach is very efficient.

This paper introduces Collaborative Contact-basedWatchdog (CoCoWa) as a new scheme for detecting selfishnodes that combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contactoccurs. This way, 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. Although some of the aforementioned papers (such as [3], [28]) introduced some degree of collaboration on their watchdog schemes, the diffusion is very costly since they are based on periodic messagedissemination.The diffusion of information about positive or negative detections of selfish nodes introduces several issues about the reputation of the neighbour nodes. The first issue is the consolidation of information, that is, the trust about neighbour's positive and negative detections, specially when it does not match with the local watchdog detection. Another issue is the case of malicious nodes. Thus, this paper extends our previous approaches [12], [13] to also cope with malicious nodes using a reputation scheme.

In order to evaluate the efficiency of CoCoWa we first introduce an analytical performance model. We model the network as a continuous time Markov chain (CTMC) and derive expressions for obtaining the time and overhead(cost) of detection of selfish nodes under the influence of false positives, false negatives and malicious nodes. In general, the analytical evaluation shows a significant 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. Finally, the pernicious effect of malicious nodes can be reduced using the reputation detection scheme. We also evaluate CoCoWa with real mobility scenarios using well known human and vehicular mobility traces. These experimental results confirm that our approach is very

efficient. The rest of the paper is organized as follows. We firstintroduce the architecture of CoCoWa in Section 2.Section 3 discusses the characterization of contact occurrence.Then, Section 4 presents a performance model for evaluating our approach. Section 5 presents the evaluation of CoCoWa in terms of detection time and overhead using the analytical model.

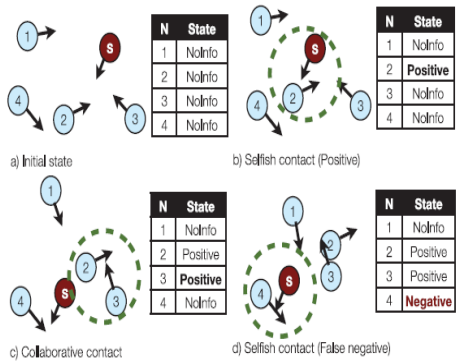

Figure 1. Working principle

2. ARCHITECTURE OVERVIEW

A selfish node usually denies packet forwarding in order to save its own resources. This behaviour implies that a selfishnode neither participates in routing nor relays data packets [21]. A common technique to detect this selfish behaviouris network monitoring using local watchdogs. A node's watchdog consists on overhearing the packets transmittedand received by its neighbours in order to detect anomalies, such as the ratio between packets received to packets being retransmitted[15]. By using this technique, the local watchdog can generate a positive (or negative) detection in case thenode is acting selfishly (or not).An example of how CoCoWa works is outlined in Fig. 1.It is based on the combination of a local watchdog and the diffusion of information when contacts 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 selfishnode, 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. Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly, through the collaborative transmissionof information that is provided by other nodes.Under this scheme, the uncontrolled diffusion of positiveand negative detections can produce the fast diffusion of wrong information, and therefore, a poor network performance.

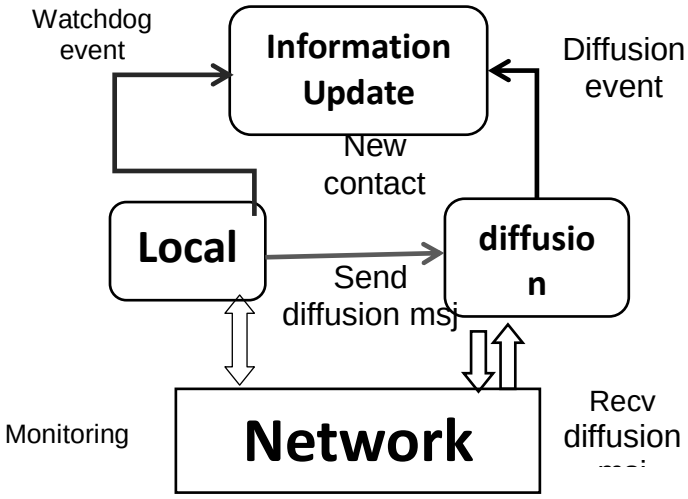

Figure 2. Block diagram

For example, in Fig. 1, on the last state d), node two and three have a positive detection and node four has a negativedetection (a false negative). Now, node one, which has no information about the selfish node, has several possibilities:if it contacts the selfish node it may be able to detect it; if it contacts node two or three it can get a positive detection;but if it contacts node four, it can get a false negative. Fig. 2 shows the functional structure of CoCoWa and wenow detail its three main components.The Local Watchdog has two functions: the detection ofselfish nodes and the detection of new contacts.

The local watchdog can generate the following events about neighbournodes: PosEvt (positive event) when the watchdog detects a selfish node, NegEvt (negative event) when thewatchdog detects that a node is not selfish, and NoDetEvt (no detection event) when the watchdog does not have enough information about a node (for example if the contact time is very low or it does not overhear enoughmessages). The detection of new contacts is based on neighbourhood packet overhearing; thus, when the watchdogoverhears packets from a new node it is assumed tobe 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 (and negative) detections.

A key issue of our approach is the diffusion of information.As the number of selfish nodes is low compared tothe total number of nodes, positive detections can always be transmitted with a low overhead. However, transmittingonly positive detections has a serious drawback: false positives can be spread over the network very fast. Thus, thetransmission of negative detections is necessary to neutralize the effect of these false positives, but sending all knownnegative detections can be troublesome, producing excessive messaging or the fast diffusion of false negatives. Consequently,we introduce a negative diffusion factor g, that isthe ratio of negative detections that are actually transmitted.This value ranges from 0 (no negative detections are transmitted)to 1 (all negative detections are transmitted). We will show in the evaluation section that a low value for the g factor is enough to neutralize the effect of false positivesand false negatives. Finally, when the diffusion module receives a new contact event from the watchdog, it transmits a message including this information to the new neighbor node. When the neighbor node receives a message, it generatesan event to the network information module with the list of these positive (and negative) detections.Updating or consolidating the information is another key issue. This is the function of the Information Update module.A node can have the following internal information about other nodes: NoInfo state, Positive state and Negative state. A NoInfo state means that it has no information about a node, a Positive state means it believes that a node is selfish, and a Negative state means it believes that a node is not selfish. A node can have direct information (from the local watchdog) and indirect information (from neighbor nodes). CoCoWa is event driven, so the state of anode is updated when the PosEvt or NegEvt events are received from the local watchdog and diffusion modules.

The advantages of this updating strategy are twofold.First, with the threshold u we can reduce the fast diffusion of false positive and false negatives. Nevertheless, this can produce a delay on the detection (more events are neededto get a better decision). Second, the decision about a selfish node is taken using the most recent information. For example,if a node had contact with the selfish node a long time ago (so it had a Positive state) and now receives severalNegEvt in a row from other nodes, the state is updated toNegative.Finally, the network information about the nodes has an expiration time, so after some time without contacts it is updated.

3. THE MODEL FOR THE COCOWA ARCHITECTURE

The goal of this section is to model the behaviour of the differentmodules of our architecture (see Fig. 2). The local watchdog is modelled using three parameters: the probabilityof detection p_d, the ratio of false positives p_{fp}, and the ratio of false negatives p_{fn}. The first parameter, the probabilityof detection (p_d), reflects the probability that, when a node contacts another node, the watchdog has enoughinformation to generate a PosEvtor NegEvtevent. This value depends on the effectiveness of the watchdog, thetraffic load, and the mobility pattern of nodes. For example,for opportunistic networks or DTNs where the contacts aresporadic and have low duration, this value is lower than for MANETs. Furthermore, the watchdog can generate falsepositives and false negatives. A false positive is when the watchdog generates a positive detection for a node that is not a selfish node. A false negative is generated when a selfish node is marked as a negative detection The diffusion module can generate indirect events when a contact with neighbour nodes occurs. Nevertheless, a contactdoes not always imply collaboration, so we model this probability of collaboration as pc. The degree of collaborationis a global parameter, and it is used to reflect that either a message with the information about the selfish node islost, or that a node temporally does not collaborate (for example, due to a failure or simply because it is switchedoff). In real networks, full collaboration (pc ¼ 1) is almost impossible. Finally, the probability of generating the indirectevents are the following_ PosEvt event: a contact with another node that has aPositive state of the selfish nodewith probability pc._ NegEvt event: a contact with another node that has aNegative state, being the probability g _ pc. Notethatnot all Negative states are transmitted, itdepends on the diffusion factor g.The information update module is driven by the previouslocal and indirect events. These events update the reputation r about a node, and are used to finally decide if a nodeis selfish or not using the threshold u.4.2 Malicious Nodes and Attacker ModelMalicious nodes attempt to attack the CoCoWa system by generating wrong information about the nodes. Thus, theattacker model addresses the behaviour or capabilities of these malicious nodes. A malicious node attack consists of trying to send a positive about a node that is not a selfish node, or a negative about a selfish node, with the goal of producing false positives and false negatives on the rest of nodes. In order to do this, it must have some knowledgeabout the way CoCoWa works. The effectiveness of this behaviour clearly depends on the rate and precision thatmalicious nodes can generate wrong information. Malicious nodes are assumed to have a communications

hardwaresimilar to the rest of nodes, so they can hear all neighbor messages in a similar range than the rest of nodes. Nevertheless,the attacker could use high-gain antennas to increase its communications range and thus disseminatefalse information in a more effective manner

4. ANALYTICAL EVALUATION

This section is devoted to evaluate the performance of CoCoWa. The analytical model introduced in Section 4 hasseveral parameters, so in this paper we focus on those parameters that clearly affect performance. First, we studythe global performance of our approach considering the collaborative issues. Then, we focus our study on the impact offalse negatives, false positives, and malicious nodes. Finally, we compare our approach to the classic periodic diffusion model. Note that, since _ is a multiplying factor of all transition rates in matrix Q (except for qii), the concluding resultsof this section are valid for any value of _ (a greater value of will affect only on a reduction of the detection time). Forthe evaluations that follow, we consider a _ value of 0.01 contacts/s, which has been shown to be a valid value in vehicularscenarios [37]. The following evaluations also consider the experimental ranges of several parameters obtainedfrom previous works of our research group [16], [29]. In particular,the probability of detection is low because the localwatchdog needs enough packets to generate a positive (or negative) detection of a selfish node pd ½0:1; 0:3, and theratio of false negatives and false positives are related to pd; for the range considered the former take the following values:pfn ½0:05; 0:25 and pfp ½0:1; 0:3

5. SELFISH MISBEHAVIOR MODEL

In a network, normal nodes follow network protocols to transmit or receive messages, while selfish nodes manipulatetheir local protocols in order to achieve higher performance (e.g., throughput). We classify selfish nodes into twotypes: dumb selfish nodes and smart selfish nodes. Dumb selfish nodes are aggressive and just aim to gain higher performance.Smart selfish nodes, however, are more cautious and intend to obtain better performance without gettingbusted by normal nodes. For instance, smart selfish nodes can learn normal nodes' detection schemes and change theirown behavior adaptively. Comparing these two types of selfish nodes, we can easily see that dumb selfish nodes are much easier to detect than smart ones. In this study, we will first develop a general detection scheme for both kinds ofselfish nodes and then propose some defense mechanisms to make sure that smart selfish nodes cannot affect normal nodes' performance without getting caught. Note that most previous detection schemes do not discuss what to do withthe selfish nodes after detecting them. In this paper, we employ a simple penalty scheme to punish the detected selfish nodes, which is to let all their one-hop neighbors stop forwarding packets for them until they receive a notice indicatingthat these nodes are not selfish any more.Besides, in this work we study MAC layer selfish misbehavior in IEEE 802.11 ad hoc networks. In such networks,selfish nodes can manipulate the following MAC layer parameters to enhance their channel access probability:duration of the rest of the transmission (or the remaining transmission duration), SIFS duration, DIFS duration, and backoff time. Specifically, when sending RTS or DATA frames, by increasing the included duration value, a selfish node can claim to occupy the channel for a longer period to

prevent other normal nodes from contending for the channel.A selfish node may also choose a smaller SIFS duration so asto finish its current transmission sooner to initiate the next one. In addition, by setting DIFS to a smaller value after sensing the channel idle, a selfish node will wait a shorter timeinterval to start the backoff process and may have higher channel access probability. Moreover, when manipulatingbackoff time, selfish nodes may employ many different strategies in order to gain higher channel access probability. Weconsider three typical strategies herein as follows:

Naive strategy. A selfish node always chooses a smallconstant value as its backoff time.Random strategy. Instead of cbackoff time, a selfish noderandomlychooses itsbackoff time from a smaller fixed contention windowthan that of normal nodes, for example, ½0; CWmin=4_.Thus, the selfish node's expected backoff period is-smaller than that of normal nodes._ g-Persistent strategy. Instead of choosing a fixed contentionwindow size, a selfish node still follows the IEEE BEB rule to double its contention window sizein case of retransmissions. However, its backoff time is determined by multiplying a randomly chosenvalue in current contention window by a control parameter g (0 _ g _ 1), i.e., TB ¼ tb _ g where TB isthe backoff time and tbis the randomly chosen value in current contention window.Note that the proposed detection scheme can be used to detect selfish nodes employing any strategies. We consider the above three typical selfish strategies when designing defense schemes against smart selfish nodes. The detection and defense schemes are carried out by observers, i.e.,neighbors of the node of interest, and coordinated by local cluster heads who are known to be honest. For instance, the local

Simulation time	Delay/sec		Throughput/per time		Efficiency False-Positive		Efficiency False-Negative	
	Without detection COCOWA	With detection COCOWA	Without detection COCOWA	With detection COCOWA	Without detection COCOWA	With detection COCOWA	Without detection COCOWA	With detection COCOWA
100	-	-	71680	114240	0.093533	0.09986 11	0.09 13455	0.08 48374
150	-	-	151040	194240	0.093269	0.09 99154	0.08 272 44	0.07 53961
200	0.107267	0.037646 4	231680	274240	0.092253	0.09 99259	0.07 657 72	0.06 94778
250	0.087810 2	0.036560 4	311680	354240	0.09 9094	0.09 993 47	0.07 271 26	0.06 57819
300	0.075665	0.035005 3	391680	434240	0.090641	0.09 994 39	0.07 010 43	0.06 33226

Table 1. Comparison function of the CoCoWa techniques

cluster heads can be determined based on nodes' longterm behavior histories.

6. SELFISH MISBEHAVIOR DETECTION

In this section, we propose to detect selfish misbehavior through normal nodes' observations. Specifically, we considera multi-hop wireless network working on a single channel, in which every node is watched by all its neighbors.Normal nodes will compare the observed data with their counterparts under normal protocol operations, andapply the detection rules to determine whether the node under observation is a selfish node or not. Recall that inIEEE 802.11 networks, selfish nodes can manipulate four MAC layer parameters to gain higher channel access probability:the remaining transmission duration, SIFS duration,DIFS duration, andbackoff time.

7. SIMULATION RESULTS

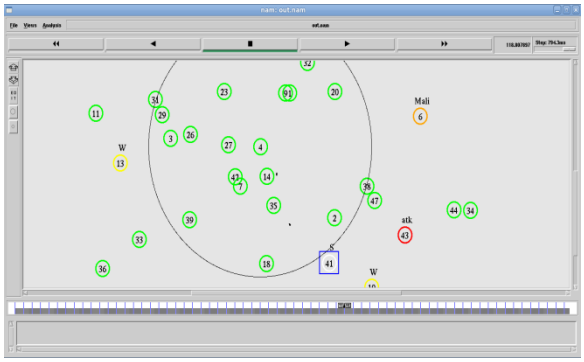

Figure 3. Sending of data from source node

Here 41node indicate that it is a source node.the data is sending from that node

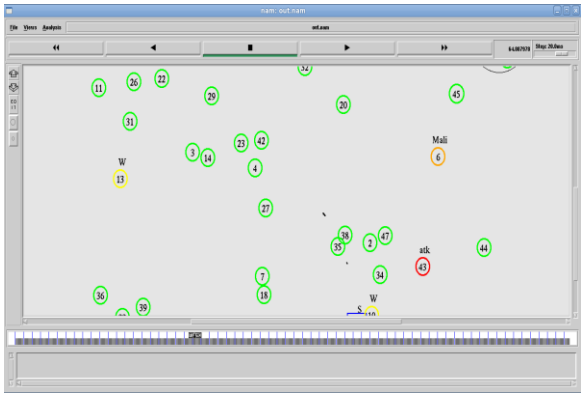

Figure 4. Analyzing the data with the reference nodes

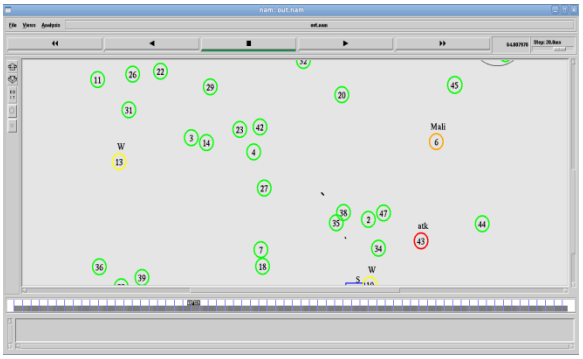

Figure 5. Detecting the selfish node

CONCLUSION

This paper proposes 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. Cocowa is based on the diffusion of the known positive and negative detections. When a contact occurs between two collaborative nodes, the diffusion module transmits and processes the positive (and negative) detections.

In short, the combined effect of collaboration and reputation of our approach can reduce the detection time while increasing the global accuracy using a moderate local precision watchdog.based on the proposed detection scheme, we design three defense schemes against three typical kinds of selfish nodes manipulating their back off times, i.e., naive selfish nodes, random selfish nodes, and g-persistent selfish nodes. In particular, a naive selfish node always chooses a small constant value as its back off time. A random selfish node randomly chooses its back off time from a smaller fixedcontention window than that of normal nodes. A g-persistent selfish node still follows the IEEE 802.11 BEB rule to double its contention window size in case of retransmissions. However, the back off time will be determined by multiplying a randomly chosen value in current contention window by a control parameter g. Observers can tell which kind of selfish node a node would be by monitoring its transmissions. Besides, we consider these selfish nodes smart in the sense that they aim to gain more channel access under the condition that they do not get caught by the observers (due to the penalty scheme), whose primary objective is to prevent selfish nodes from causing damage to the network. Under the proposed defense scheme, wefind that the selfish nodes cannot degrade normal nodes' performancemuch without getting detected.

REFERENCES

[1] Enrique Hern_andez-Orallo, CoCoWa: "A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes" Member, IEEE, Manuel David Serrat Olmos, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, Member, Jun 2015.

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

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

[4] Buttyan.L 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–[5] Buttyan.L and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," Mobile Netw. Appl., vol. 8, pp. 579–592, 2003.

[5] Cai.H and Eun.D.Y, "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.

[6] Chaintreau.A, P. Hui, Crowcroft.J, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on opportunistic forwarding algorithms," IEEE Trans. Mobile Comput., vol. 6, no. 6, pp. 606–620, Jun. 2007.

[7] Douceur.J.R, "The sybil attack," in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., 2002, pp. 251–26[0.

[8] Eidenbenz.S, G. Resta, and P. Santi, "The COMMIT protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes," IEEE Trans. Mobile Comput., vol. 7, no. 1, pp. 19–33, Jan. 2008.

[9] Gao.W, 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. Compute., 2009, pp. 299–308.

[10] Groenevelt.R, P. Nain, and G. Koole, "The message delay in mobile ad hoc networks," Perform. Eval., vol. 62, pp. 210–228, Oct. 2005.

[11] Hernandez-Orallo.E, 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.

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