**International Journal of Advanced Research and Interdisciplinary Scientific Endeavours, Vol. 2(4), 2025**
**DOI: 10.61359/11.2206-2519**

# An Efficient Approach to Identifying Selfish Nodes in MANETs and DTNs

V. Gowsalya*

Email Correspondence*: gowsi.aaris@gmail.com

[1] Assistant Professor, Department of Electronics and Communication, Sri Raaja Raajan College of Engineering and Technology, Amaravathipudur, Tamil Nadu, India.

## Abstract:

Mobile ad-hoc networks (MANETs) assume that mobile nodes voluntarily cooperate in order to work properly. This cooperation is a cost-intensive activity, and some nodes can refuse to cooperate, leading to selfish node behaviour. Thus, the overall network performance could be seriously affected. The use of watchdogs is a well-known mechanism to detect selfish nodes. However, the detection process performed by watchdogs can fail, generating false positives and false negatives that can induce wrong operations. Moreover, relying on local watch dogs alone can lead to poor performance when detecting selfish nodes, in terms of precision and speed. This is especially important on networks with sporadic contacts, such as delay tolerant networks (DTNs), where sometimes watchdogs lack enough time or information to detect selfish nodes. Thus, we propose collaborative contact-based watchdog (CoCoWa) as a collaborative approach based on the diffusion of local selfish nodes awareness when a contact occurs, so that information about selfish nodes is quickly propagated. As shown in the paper, this collaborative approach reduces the time and increases the precision when detecting selfish nodes.

**Keywords:** Wireless Networks, Manets, Opportunistic and Delay Tolerant Networks, Selfish Nodes.

## 1. 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 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 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 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. Literature provides two main strategies to deal with 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. These approaches are usually based on virtual currency and/or game theory models The detection and exclusion approach are a straight-forward way to cope with selfish nodes and several solutions have been presented.

[*] Assistant Professor, Department of Electronics and Communication, Sri Raaja Raajan College of Engineering and Technology, Amaravathipudur, Tamil Nadu, India.

**Article Timeline:** Received: Apr 16, 2025; Revised: Apr 28, 2025; Published: Apr 30, 2025

## 2. Previous Design Problem

In CoCoWa, we do not attempt to implement any strategy to exclude selfish nodes or to their participation; instead, we focus on the detection of selfish nodes. The impact of node selfishness on MANET init is shown that when no selfishness prevention mechanism is present, the packet delivery rates become seriously degraded, from a rate of 80 percent when the selfish node ratio is 0, to 30 percent when the selfish node ratio is 50 percent. The survey shows similar results: the number of packet losses is increased by 500 percent when the selfish node ratio increases from 0 to 40 percent. A more detailed study shows that a moderate concentration of node selfishness (starting from a 20 percent level) has a huge impact on the overall performance of MANETs, such as the average hop count, the number of packets dropped, the offered throughput, and the probability of reach ability. In DTNs, selfish nodes can seriously degrade the performance of packet transmission. For example, in two-hop relay schemes, if a packet is transmitted to a selfish node, the packet is not re-transmitted, therefore being lost. 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. 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 behavior from the network. Thus, since we assume that these nodes may be present on the network, evaluating their influence becomes a very relevant matter.

## 3. Proposed System

In this paper introduces Collaborative Contact-based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes 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 contact occurs. This way, nodes have secondhand 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 introduced some degree of collaboration on their watchdog schemes, the diffusion is very costly since they are based on periodic message dissemination.

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 in the neighbour's positive and negative detections, especially when it does not match the local watchdog detection. Another issue is the case of malicious nodes. Thus, this paper extends our previous approaches 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.

## 4. Design Module

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.

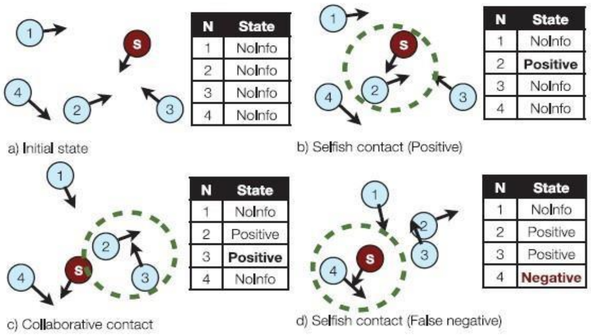


**Figure-1 An example of how CoCoWa works.**

**a) Initially all nodes have no information about selfish nodes. 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).**

By using this technique, the local watchdog can generate a positive (or negative) detection incase the node 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 occur. 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 these positive (or negative) detections. Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly, through the collaborative trans-mission of information that is provided by other nodes. Under this scheme, the uncontrolled diffusion of positive and negative detections can produce the fast diffusion of wrong information, and therefore, poor network performance.

## 5. Architecture Overview

The Local Watchdog has two functions: the detection of selfish nodes and the detection of new contacts. The local watchdog can generate the following events about neigh-bour nodes: 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 does not have enough information about a node (for example if the contact time is very low or it does not overhear enough messages). The detection of new contacts is based on neighborhood packet overhearing; thus, 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.

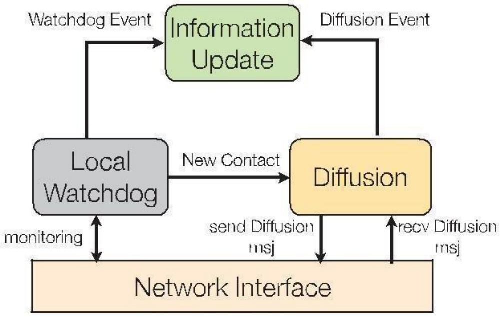


**Figure-2 CoCoWa Architecture.**

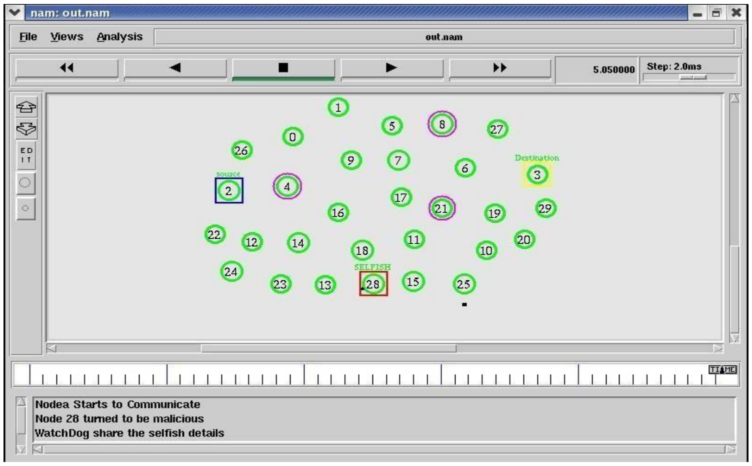
Fig. 2 shows the functional structure of CoCoWa and we now detail its three main components.

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 to the total number of nodes, positive detections can always be transmitted with a low overhead. However, transmitting only positive detections has a serious drawback: false positives can be spread over the network very fast. 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.

Consequently, we introduce a negative diffusion factor, that is the ratio of negative detections that are actually transmitted. This value ranges from 0 (no negative detections are trans-mitted) 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 neutralise the effect of false positives and 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 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.

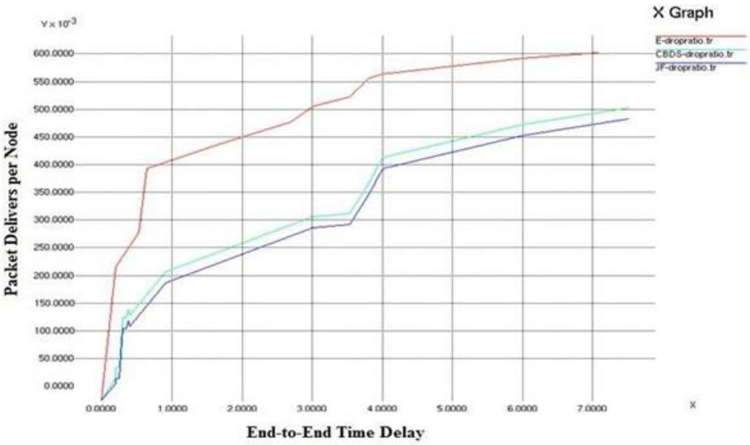
Updating or consolidating the information is another key issue. This is the function of the Information Update module. A node can have the following internal information about other nodes: NoInfo state, Positive state and Negative state. A NoInfo state means that it has no information about a node, a 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 neighbour nodes). 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.

## Simulation Results

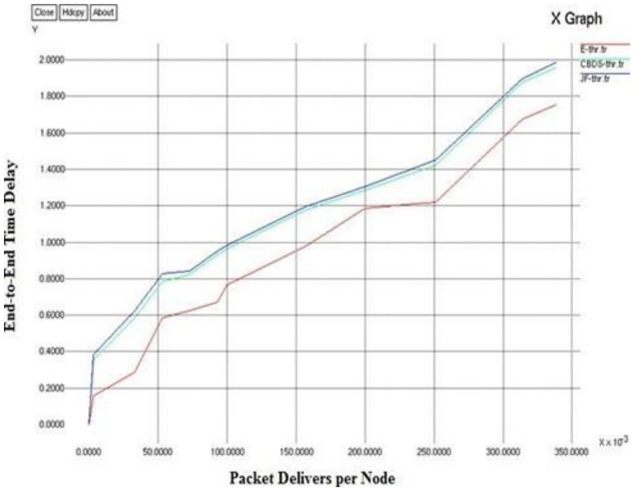


Nodea Starts to Communicate
Node 28 turned to be malicious
WatchDog share the selfish details

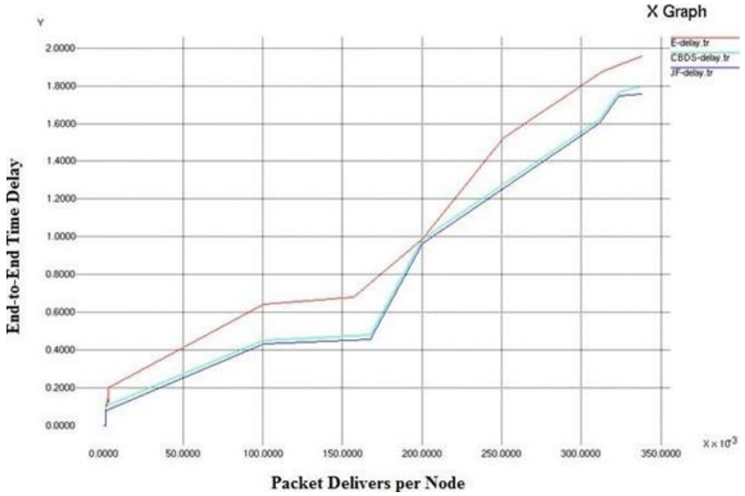
## DROP RATIO



## THRESOLD



## DELAY



## 7. Related Work

There are two main strategies to deal with selfish behaviour in cooperative networks. The first approach tries to motivate the nodes to actively participate in the forwarding activities. For example, in the authors presented a method using a virtual currency called nuglet. Zhonget al. pro-posed SPRITE, a credit-based system to incentive participation of selfish nodes in MANET communication. These incentivation methods present several problems, such as the need for some kind of implementation infrastructure to maintain accounting and they usually rely on the use of some kind of tamper- proof hardware.

The COMMIT Protocol combines game-theoretic techniques to achieve truthfulness and an incentivation payment scheme to reduce the impact of selfish nodes on routing protocols. Regarding the detection and exclusion approach, there are several solutions for MANETs and DTNs. A first study about misbehaving nodes and how watchdogs can be used to detect them was introduced. The authors proposed a Watchdog and Path rater over the DSR protocol to detect non-forwarding nodes, maintaining a rating for every node. In another scheme for detecting selfish nodes based on context aware information was proposed.

In previous works it has been shown how some degree of cooperation can improve the detection of selfish or misbehaving nodes. The CONFIDENT protocol was proposed in, which combines a watchdog, reputation systems, Bayesian filters and information obtained from a node and its neighbours to securely detect misbehaving nodes. The system's response is to isolate those nodes from the network, punishing then indefinitely. A distributed intrusion detection system (IDS) is introduced . In this approach, if a node detects an intrusion with strong evidence, it can initiate a response. However, if a node detects an anomaly with weak evidence, it can initiate a cooperative global intrusion detection procedure.

A similar approach is the mobile intrusion detection system described. In this case, local sensor ratings are periodically flooded throughout the network in order to obtain a global rating for each misbehaving node. Another approach is CORE "collaborative reputation mechanism". The CORE system is similar to the distributed IDS approaches described below. It consists in local observation using watchdogs that are combined and distributed to obtain a reputation for each node.

## 8. Conclusion

This paper proposes CoCoWa as a collaborative contact-based watchdog to reduce 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. Analytical and experimental results show that CoCoWa can reduce the overall detection time with respect to the original detection time when no collaboration scheme is used, with a reduced overhead (message cost). This reduction is very significant, ranging from 20 percent for very low degrees of collaboration to 99 percent for higher degrees of collaboration. Regarding the overall precision we show how by selecting a factor for the diffusion of negative detections, the harmful impact of both false negative and false positives is diminished. Finally, using CoCoWa we can reduce the effect of malicious or collusive 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, we have shown that 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. 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.

## 7. References

[1] Zhao, X., & Han, Z. (2017). "Detecting selfish behaviors in Delay Tolerant Networks through collaborative approaches." Proceedings of the International Symposium on Wireless Communication Systems (ISWCS 2017), 1-6.

[2] Khan, F., & Bhatti, A. (2016). "A survey on detection techniques for selfish behavior in wireless ad hoc networks." International Journal of Computer Science and Information Security, 14(9), 588- 594.

[3] Patel, S., & Verma, A. (2012). "Game theory-based approach for selfish node detection in mobile ad hoc networks." International Journal of Computer Science and Mobile Computing, 1(5), 281- 288.

[4] Khalil, I., & Shah, M. (2015). "Mitigation of selfish nodes in mobile ad hoc networks." International Journal of Computer Applications, 123(10), 17-23.

## 8. Conflict of Interest

The authors declare that there are no conflicts of interest to report in the publication of this article.

## 9. Funding

No external funding was received to support or conduct this study.