**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 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 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 is a straight-forward way to cope with selfish nodes and several solutions have been presented In CoCoWa, we do not attempt to implement any strategy to exclude selfish nodes or to incentivize their participation; instead, we focus on the detection of selfish nodes. In CoCoWa, we do not attempt to implement any strategy to exclude selfish nodes or to incentivize their participation; instead, we focus on the detection of selfish nodes.

The impact of node selfishness onMANETs has been studied. In it 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 [30] 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 reahability. 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. Essentially, watchdog systems overhear wireless traffic and analyses it to decide whether neighbor 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 behavior of the system.

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 a contact occurs. 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 introduced some degree of collaboration on their watchdog schemes, the diffusion is very costly since they are based on periodic message dissemination.

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.

**ARCHITECTURE OVERVIEW**

A selfish node usually denies packet forwarding in order to save its own resources. This behavior implies that a selfish node neither participates in routing nor relays data packets. A common technique to detect this selfish behavior 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 retransmitted. By using this technique, the local watchdog can generate a positive (or negative) detection in case the node is acting selfishly.

**RELATED WORK**

There are two main strategies to deal with selfish behavior 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. Zhong et al. proposed SPRITE, a credit-based system to incentivate 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 the 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 Pathrater 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 locally 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.