International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 36 • 2017

Selfish and Malicious Node Behavior Pattern using Chord Algorithm

K. Vinodh kumar[a] and S. Padmapriya[b]

[a]*Department of Information Technology,, Research scholar, St.Peter's University, Chennai, Tamilnadu, India*

E-mail: vinodhkumarit@gmail.com

[b]*Department of Information Technology, , Professor / CSE, Prathyusha Engineering College, Tamilnadu, India*

E-mail: padmapriya.sha@gmail.com

Abstract: It hides the Source node identities to the destination node within networks. Existing anonymity routing protocols in MANETs are classified into two categories: hop-by-hop encryption and redundant traffic, Most of the recent approaches are limited by focused on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost.

Keywords: *Mobile Ad hoc Network, Vehicular Ad hoc Networks, Delay tolerant Networks, Node Behavior, Collaborative Contact-based Watchdog (CoCoWa), 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 application 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. The literature provides two main strategies to deal with selfish behaviour: (*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.

1.1. Problem Definition

DTNs to deal with find out the malicious, selfish misbehaving nodes and genuine loss nodes. Selfishness is social selfishness, as very often humans carrying communication devices in a DTN are socially selfish to outsiders but unselfish to friends. Maliciousness refers to malicious nodes performing trust-related attacks to disrupt DTN operations built on trust. We aim to identify the malicious node and selfish node based on checking node energy level and buffer level using multi hop forwarding algorithm. But it is time consuming process.

1.2. Problem Statement

ALERT can be used to different network models with various node movement patterns such as random waypoint model and group mobility. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to decrease the communication latency. The location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, an unknown communication protocol that can provide intractability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field.

2. RELATED WORK

2.1. An Iterative Algorithm For Trust Management And Adversary Detection For Delay Tolerant Networks

Delay/Disruption Tolerant Networks (DTNs) have been identified as one of the key areas in the field of wireless communication,where in sparseness and delay are particularly high. They are emerging as a promising technology in vehicular, planetary/interplanetary,military/tactical, disaster response, underwater and satellite networks. DTNs are characterized by large end-to-end communication laten cyand the lack of end-to-end path from a source to its destination.

These characteristics pose several challenges to the security of DTNs. Especially, Byzantine attacks in which one or more legitimate nodes have been compromised and fully controlled by the adversary can give serious damages to the network in terms of latency and data availability. Using reputation-based trust management systems is shown to bean effective way to handle the adversarial behavior in Mobile Ad-hoc Networks (MANETs).

Applying ITRM to DTNs for various mobility models, we observed that the proposed iterative reputation management scheme is far more effective than well-known reputation management techniques such as the Bayesian framework and EigenTrust. Further, we concluded that the proposed scheme provides high data availability and packet-delivery ratio with low latency in DTNs under various adversary attacks which attempt to both undermine the trust and detection scheme and the packet delivery protocol.

2.2. Dynamic Quota-Based Admission Control With Sub-Rating In Multimedia Servers

An admission control algorithm for a multimedia server is responsible for determining if a new request can be accepted without violating the Quality of Service (QoS) requirements of the existing requests in the system. A novel quota-based admission control algorithm with sub-rating for two priority classes of requests is proposed in this study.

The server capacity is divided into three partitions based on the quota values: one for each class of requests and one common pool shared by two classes of requests. Reward and penalty are adopted in the proposed system model. High-priority requests are associated with higher values of reward as well as penalty than low-priority ones. Given the characteristics of the system workload, the proposed algorithm finds the best partitions, optimizing the system performance based on the objective function of the total reward minus the total penalty. The sub-rating mechanism will reduce the QoS requirements of several low- priority clients, by cutting out a small fraction of the assigned server capacity, to accept a new high priority client and to achieve a higher net earning value.

Astochastic Petri-Net model is used to find the optimal quota values and two approximation approaches are developed to find sub-optimal settings. The experiment results show that the proposed algorithm performs better than one without subrating mechanism, and that the sub-optimal solutions found by the proposed approximation approaches are very close to optimal ones. The approximation approaches enable the algorithm to dynamically adjust the quota values, based on the characteristics of the system workload, to achieve higher system performance efficient in detecting possible misbehavior.

2.3. Delay-/Disruption-Tolerant Networking state Of The Art And Future Challenges

Networking for challenged environments, or Delay- and Disruption-Tolerant Networking as it is now most commonly referred to, has attracted great attention in the past few years by the networking research community.

Connectivity disruptions, limited network capacity, energy and storage constraints of the participating, mobile devices and the arbitrary movement of nodes are only a few of the challenges that the protocol stack has to deal with. Clearly, current Internet protocols (i.e., the TCP/IP protocol stack) suffer and can fail under such conditions. In this paper, we initially give the DTN Problem Statement; we contend that not all applications have the same requirements from the system and hence ,equal (blind) treatment of all data packets will result in reduced network efficiency.

Based on that we propose a Design Position for DTN protocols, which states that protocol design has to be done proactively, on the basis of the application's requirements.

We then survey the most recent contributions on the whole spectrum of Delay- and Disruption-Tolerant Networking, from the architectural and the application point of view down to the transport- and the network-layer of the emerging DTN protocol stack. We _nd that although not explicitly mentioned in most cases, research trends follow our Design Position. To the best of our knowledge this is the first study that discusses and evaluates research contributions from such a broad perspective. Finally, we highlight research challenges and open issues that require further investigation.

3. SYSTEM ANALYSIS

In Existing System the node could have a selfish behavior, being unwilling to forward packets for others. So the overall network performance could be seriously affected. Demerits: Waiting time is increased, Less data transmission rate ,Poor network performance

In Proposed System the data nodes are distributed among the cluster. Every node assigned with group of friend and enemies by themselves. There are selfish nodes and normal nodes in the cluster. Selfish node will not transmit packet to enemy nodes. It transmitted data packet only to friends list. Selfish nodes are greedy in transmit the data. So that it accepts most of the data transmission by own in the network. However, the detection process performed by watchdogs can failure, generating false positives and false negative that can induce to wrong operation.

Merits : Waiting time is decreased High data transmission rate, More effective, Increase network performance

3.1. Architecture Diagram

DTNs to deal with find out the malicious, selfish misbehaving nodes and genuine loss nodes. Selfishness is social selfishness, as very often humans carrying communication devices in a DTN are socially selfish to outsiders but unselfish to friends. Maliciousness refers to malicious nodes performing trust-related attacks to disrupt DTN operations built on trust. We aim to identify the malicious node and selfish node based on checking node energy level and buffer level using multi hop forwarding algorithm. But it is time consuming process

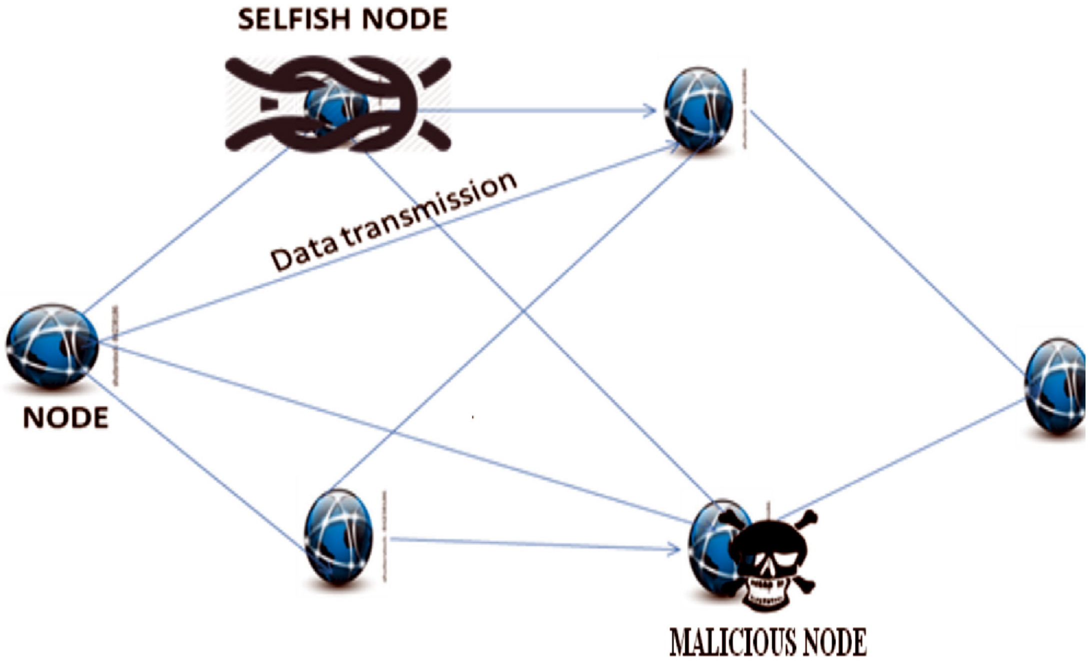


Figure 1

3.2. Forwarding Algorithm

In this scheme, The protocol has two main goals: balancing energy consumption among the DTN and forwarding the critical messages to the destination node as soon as possible. The tra□c that needs to be forwarded by a node is split into two ways one is sent to the requested DTN, the other is switch over directly to another DTN based on DTN feedback. This is chosen to minimize the overall energy consumption of the network.

4. METHODOLOGY

The network is modeled as a set of N wireless mobile nodes, with C collaborative nodes, M Malicious nodes and S selfish nodes. Our goal is to obtain the time and overhead that a set of D _ C nodes need to detect the selfish nodes in the network. The Huge number of information messages transmitted up to the detection time .Note that the following models evaluate the detection of a single selfish node. The effect of having Various selfish nodes in a network is easy to evaluate, and it not require a model. If we assume that selfish nodes are not cooperative, we can analyse the influence of each selfish node on the network independently.

4.1. The Model For The Cocowa Architecture

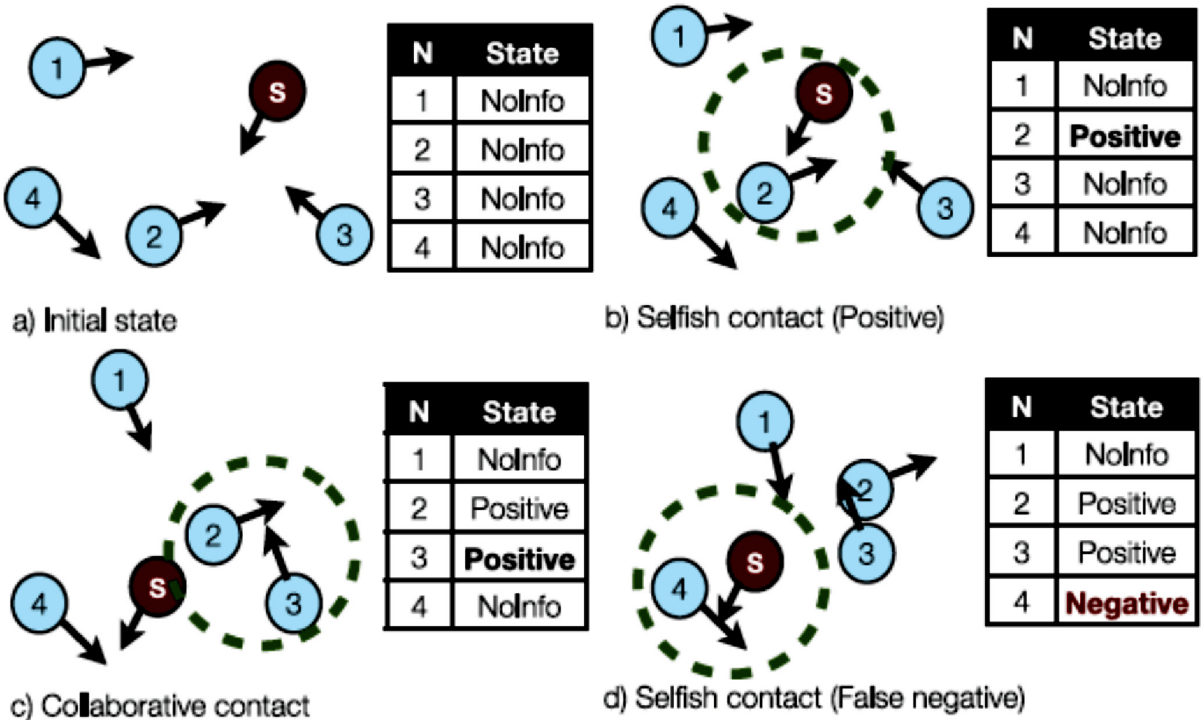
The goal of this section is to model the behaviour of the different modules of our architecture . The local watchdog is modelled using three factor the probability of detection the ratio of false positives and the ratio of false negatives The first parameter, the probability of detection reflects the probability that, when a node contacts another node, the watchdog has enough information to generate a event. This value depends on the effectiveness of the watchdog, the traffic load, and the ability to move pattern of nodes. For example for opportunistic networks or DTNs where the contacts are irregular and have low duration, this value is lower than for MANETs. Furthermore, the watchdog can generate false positives and false negatives.

4.2. Malicious Nodes And Attacker Model

Malicious nodes attempt to attack the system by generating wrong information about the nodes. Thus, the attacker model address the behaviour or efficient of these malicious nodes. A malicious node attack consists of send a positive that is not a selfish node, or a negative about a selfish node, with the goal of producing false positive and false negative on the rest of nodes. In order to do this, it must have some knowledge about the way CoCoWa works. The effectiveness of this behaviour clearly depends on the rate and Quality that malicious nodes can generate wrong information. Malicious nodes are assumed to have a communication similar to the rest of nodes, so they can hear all neighbour 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 spread false information in a more effective manner.

4.3. Collaborative Contact-Based Watchdog

In this paper we introduce Collaborative Contact-based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes that combines local watchdog detections and the spread of this information on the network. If node has previously detected a selfish node it can pass this information to other nodes when connection established. If 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 Quality by reducing the effect of both negatives and positives. Although some of the aforementioned research develops some degree of collaboration on their watchdog schemes, the diffusion is very costly since they are based on periodic message transmission. The diffusion of information about positive or negative detections of selfish nodes introduces several issues about the reputation of the neighbor nodes.



N	State
1	NoInfo
2	NoInfo
3	NoInfo
4	NoInfo

a) Initial state

N	State
1	NoInfo
2	**Positive**
3	NoInfo
4	NoInfo

b) Selfish contact (Positive)

N	State
1	NoInfo
2	Positive
3	**Positive**
4	NoInfo

c) Collaborative contact

N	State
1	NoInfo
2	Positive
3	Positive
4	**Negative**

d) Selfish contact (False negative)

Figure 2

The first issue is the consolidation of information, that is, the trust about neighbour's positive and negative detections, 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 to also cope with malicious nodes using a reputation scheme. In order to evaluate the efficiency of CoCoWa we first bring an analytical performance model. We model the network as a CONTINUOUS TIME CHAIN (CTC) and derive expressions for obtaining the time and overhead of detection of selfish nodes under the influence of false positives, false negatives and malicious nodes. In general, the analytical evaluate shows a significant reduction of the detection time of selfish nodes with a reduced cost when comparing CoCoWa against a traditional watchdog.

4.4. Network Interface

The effect of false negatives and false positives is also greatly reduced. Finally, the pernicious effect of malicious nodes can be reduced using the repeated 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 going as follows.

We first introduce the architecture of CoCoWa & discusses the characterization of contact occurrence. Then, presents a performance model for evaluating our approach. At last it presents the evaluation of CoCoWa in terms of detection time and cost using the analytical model. The CoCoWa approach is also experimentally evaluated using real mobility traces in Section 6. After presenting and evaluating our proposal we present some related work.

Updating or consolidating the information is another key issue. This is the function of the Information Update module. A node can have the internal information about other nodes: No Info state, Positive and Negative. A no information about a node, a Positive means it believes that a node is selfish, and a Negative state means it believes that a node is not selfish.

4.5. Advantage

The advantages of this updating strategy are two fold. First, with the threshold u we can reduce the fast diffusion of false positive and false negatives.

5. SYSTEM IMPLEMENTATION

5.1. Network Construction

To implement the concept, first we have to construct a network which consists of ‘n’ number of Nodes. So that nodes can receive data from other nodes in the network. We will construct the multiple network for our implementation. So that These Networks will have multiple Nodes.

5.2. Route Selection

In this module, source node broadcast the route request to destination node through all neighbor node. Based on route request destination node selects best path and forwards the route response to source through selected route neighbor nodes. Every node in network has neighbor node details for path selection and communication purpose. Each node in network has friend list.

5.3. Selfish Node Activity

In this module, every node will add their friends names in their list. Every node will spend some energy while transmitting the data in the network. This type of node will try to send the data only to its friend list nodes. If Node 1 adds Node 5 as its friend, node 1 will send the data if it transmits the data via its friend node 5 and it will not transmit the data via some other nodes. These types of nodes are named as Selfish Nodes. Due to the selfish nature and energy consuming, selfish nodes will not transmit the data to some other nodes which are not in their friends list.

5.4. Watch Dog Activity Monitoring

In this module, every nodes selfish or malicious behavior is monitored and 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. 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 or indirectly. Our main logic is to identify the best nodes through the watchdog activity monitoring.

5.5. Malicious Node Activity

As an adversary, the malicious nodes arbitrarily drop others' bundles (black hole or grey hole attack), which often take place beyond others' observation in a sparse network, leading to serious performance degradation. These types of nodes will drop the packets or divert the packets to some other nodes which are not the destination nodes. Usually malicious nodes are attacked by the attackers in a network. By this manner normal node is turned down as malicious node.

6. ALGORITHM – CHORD ALGORITHM

In this module we can verify the Neighbor nodes information of the Requested Node. So that by verifying the Id's and capacity of each neighbor node in selected route. if the neighbor node id and capacity of transferring packet mismatch means, it detects that node act as malicious node also intimate to source node. For this purpose we have to create the List of the Neighbor Nodes information for each node so that the network/ can verify the nodes request.

7. GRAPH: ANALYTICAL EVALUATION

This section is devoted to evaluate the performance of CoCoWa. The analytical model introduced in Section 4 has several parameters, so in this paper we focus on those parameters that clearly affect performance.

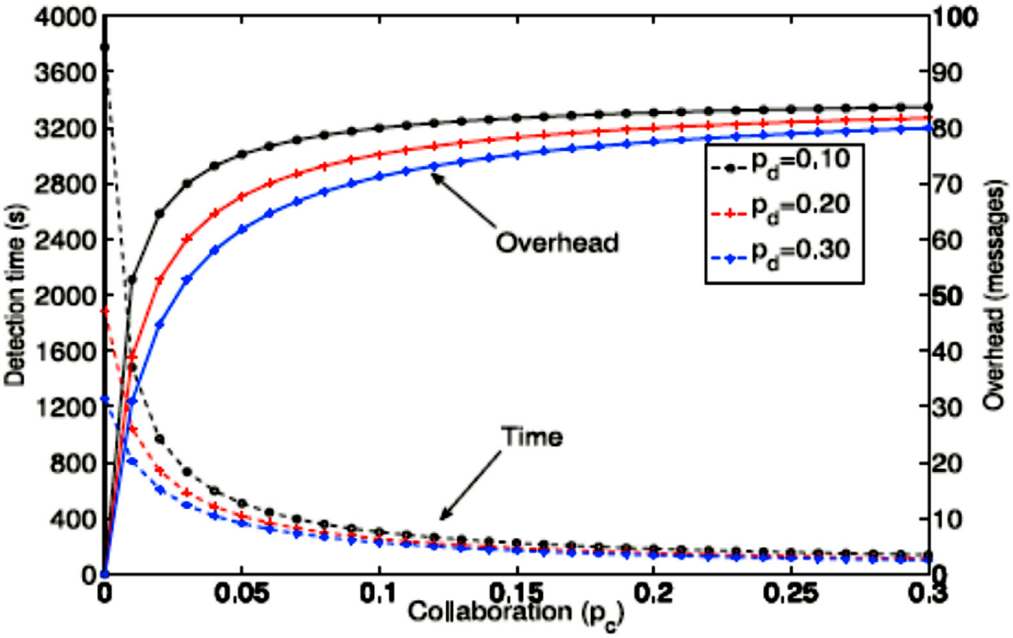


Figure 3

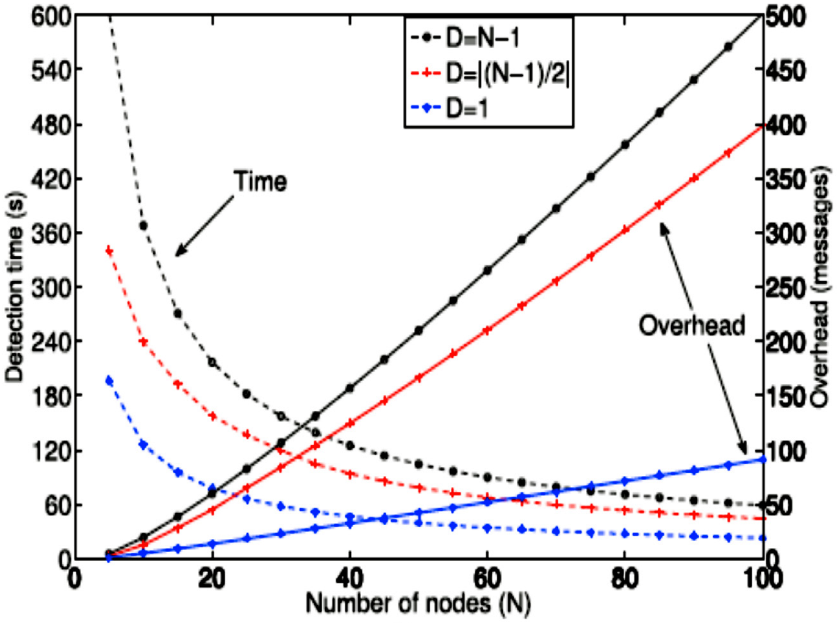


Figure 4

We observe that, when increasing the degree of collaboration from 0 to 0.2, the detection time is reduced exponentially and the overhead is increased. The effect of pd is the expected: for greater values of pd, the detection time is reduced. For example, for pd ¼ 0:1, the detection time withno collaboration (*pc* ¼ 0) is 3775 s. This value can be greatly reduced by using CoCoWa. Thus, even for a low collaborationrate (*pc* ¼ 0:2), the detection time for all nodes is reduced to 181 s with an overhead of just 82 messages, which represents an improvement of about 2000 percent on the detection time.

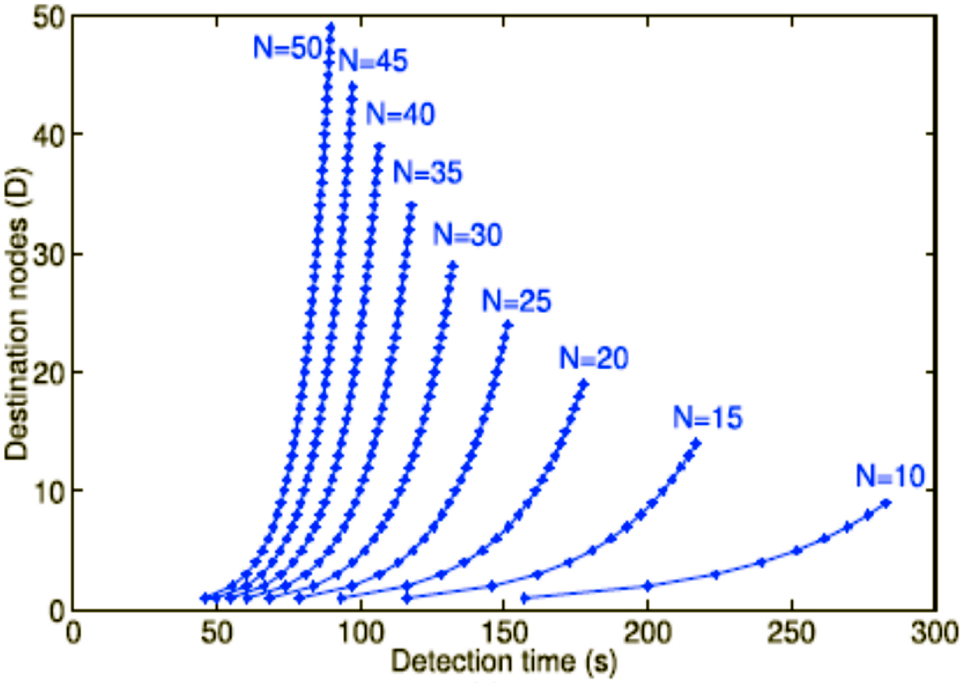


Figure 5

Regarding the detection probability (*pd*), we can see that the detection time is greatly reduced even for low values, so CoCoWa is useful in both Opportunistic Networks and DTNs. The previous results show that, when using the local watchdog alone, the detection time is very high (close to one hour). The implications are important., 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 Nnodes, thereby improving the network performance. We now evaluate the impact that the number of nodes has on performance.

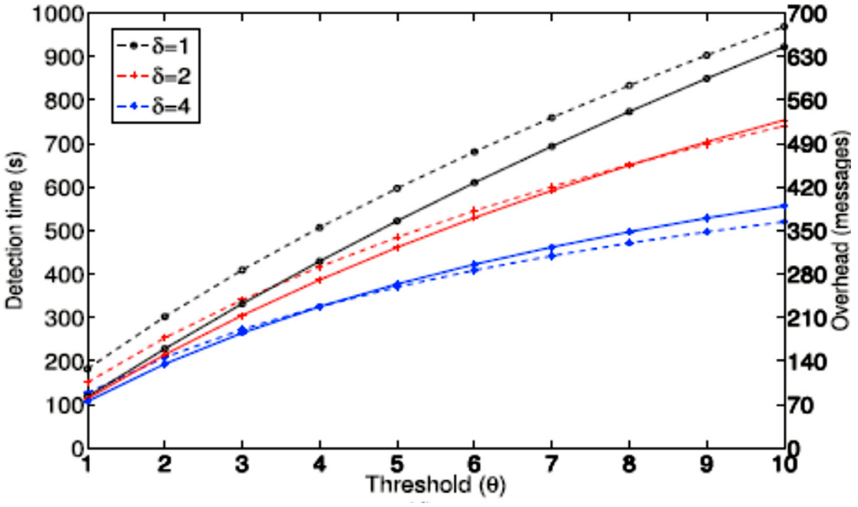


Figure 6

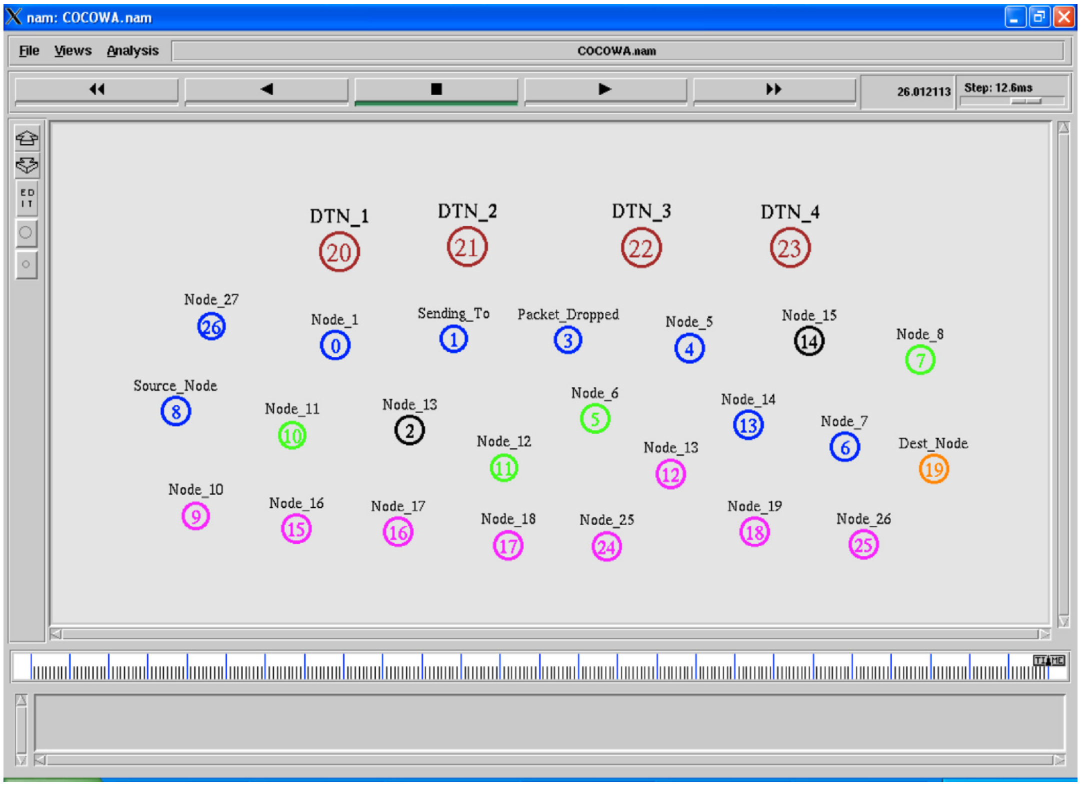


Figure 7

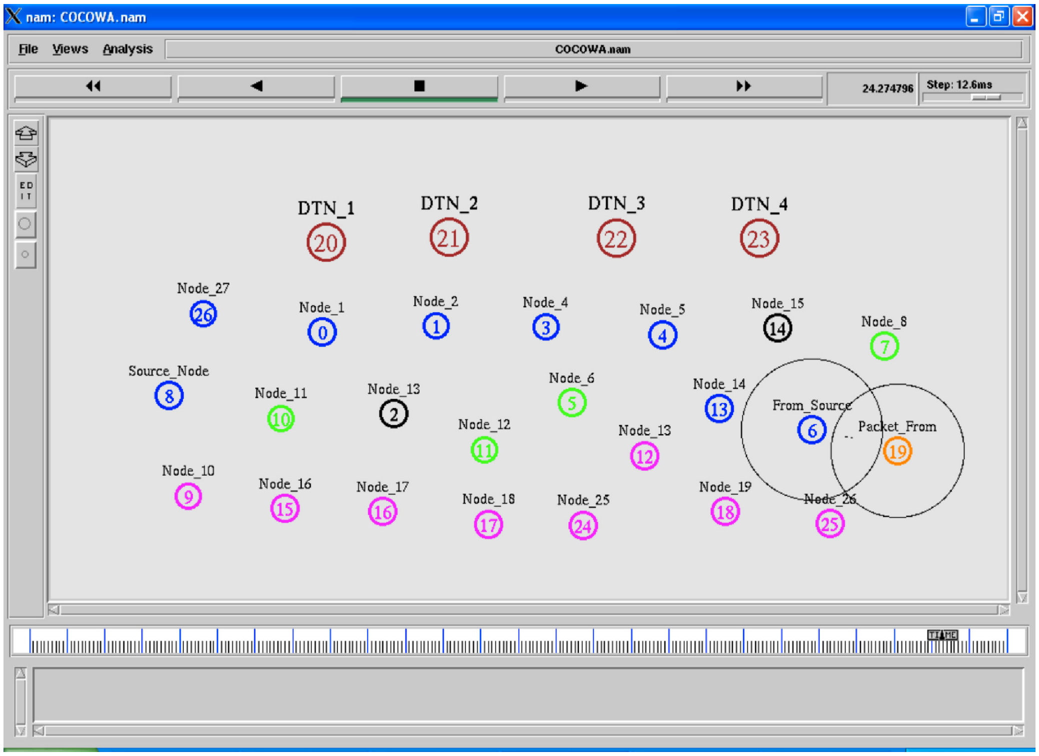


Figure 8

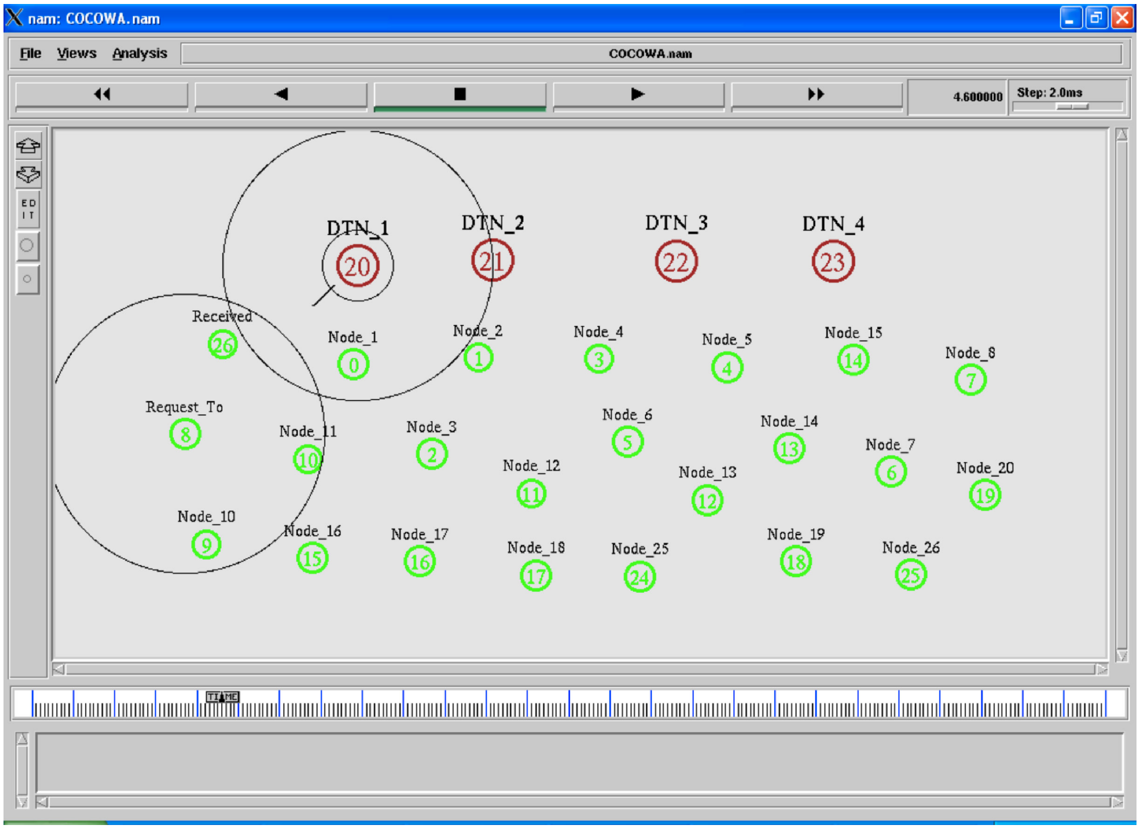


Figure 9

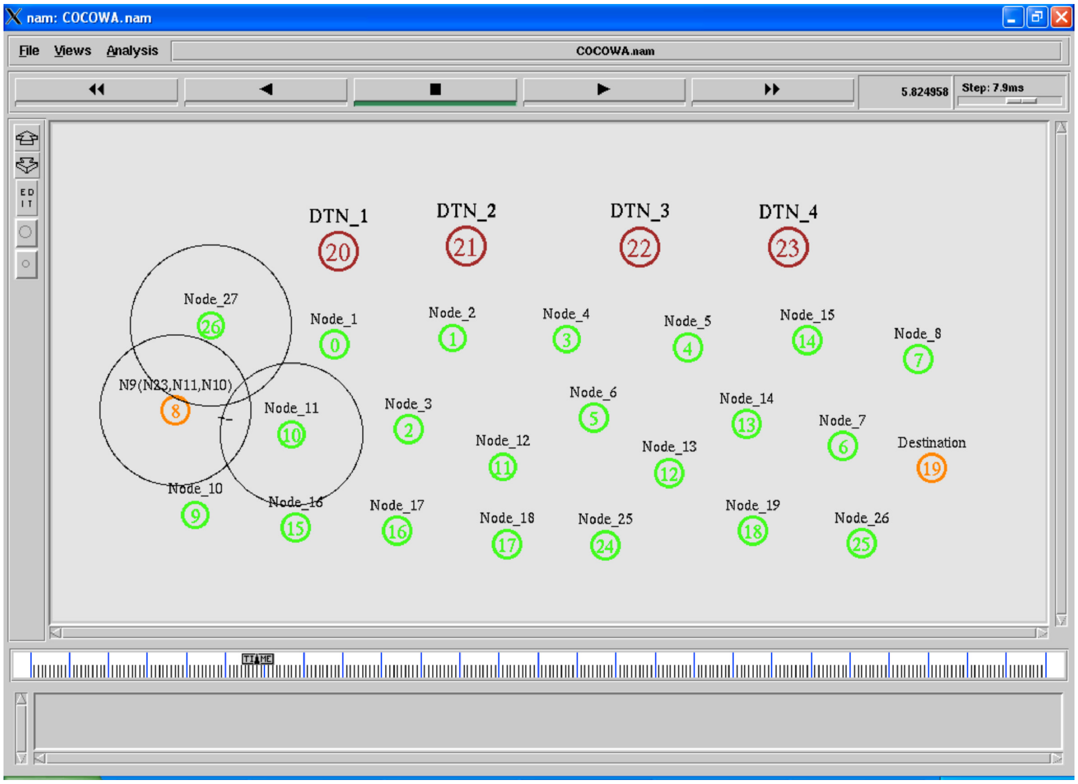


Figure 10

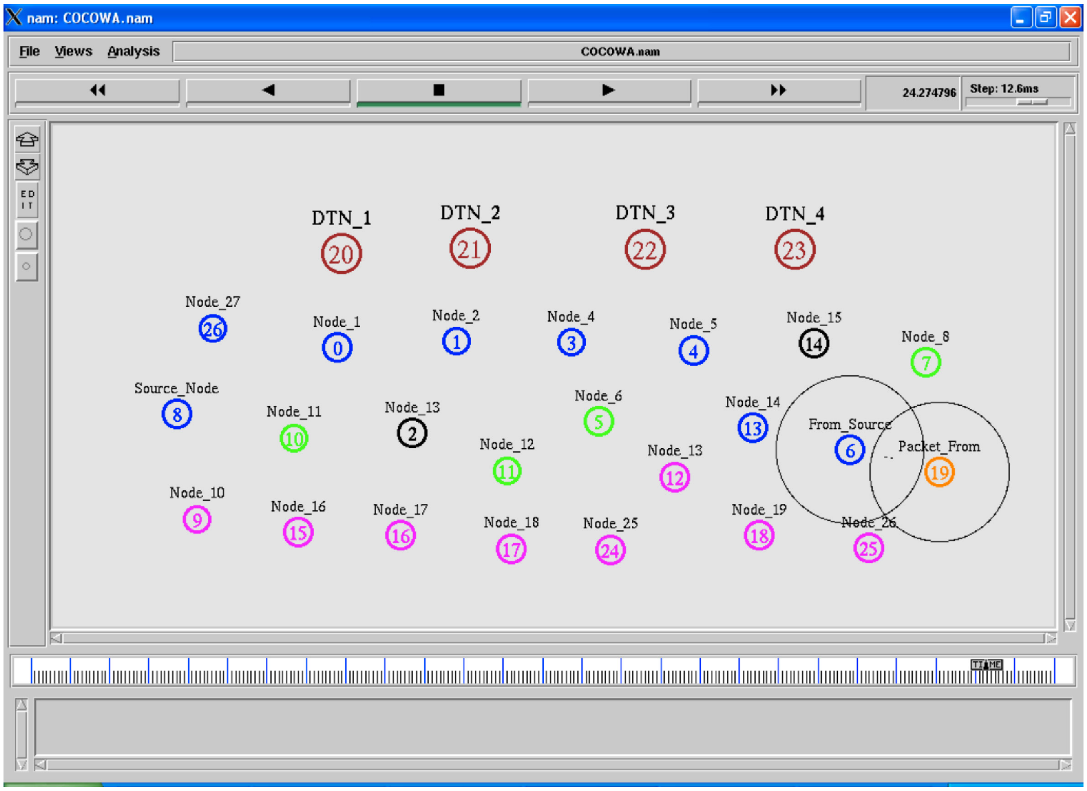


Figure 11

8. CONCLUSION

It is proposes CoCoWa as a collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish node reducing the harmful effect of false positives, false negatives and malicious nodes. CoCoWa is based on the Scatter some 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 decrease the overall detection time with respect to the original detection time when no collaboration scheme is used, with a reduced message cost. This reduction is very significant, ranging from 20 percent for very low degree 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 negatives and false positives is diminished. Finally, using CoCoWa we can reduce the effect of malicious or collusive nodes. If malicious nodes spread false negative or false positives in the network CoCoWa is able to reduce the effect of these malicious nodes fast and effectively. Additionally, we have shown that CoCoWa is also effective in opportunistic networks and DTNs, where contacts are irregular and have short durations, and where the effectiveness of using only local watchdogs can be very limited.

REFERENCE

[1] An Effective Method for Reliable Data Delivery in Highly Dynamic Mobile Ad Hoc Networks Dr. S. PadmaPriya K. Vinodh Kumar Middle-East Journal of Scientific Research 24 (2): 398-403, 2016

[2] An Unidentified Position-Based Capable Routing Protocol in Mobile Adhoc Networks S. PadmaPriya K. Vinodh Kumar international Journal of Advanced Research in Computer Science and Software Engineering Vloume5 Issues 6 1305-1309

[3] S.Padma Priya, Dr. Jayaram Pradhan, ―An Efficient security framework for detection and isolation of attacks in low rate wireless PAN , IJCSNS , Korea 2008, Vol. 8 No. 7 pp. 224-232‖

[4] Dynamic Quota-Based Admission Control With Sub-Rating In Multimedia Servers. Sheng- Cheng, Chi-Ming Chen, Ing-Ray Chen Volume 8, Issue 2, March 2000

[5] Delay-/Disruption-Tolerant Networking state Of The Art And Future Challenges Ioannis Psaras1, Lloyd Woodb , Rahim Tafazolli1 Preprint submitted to Elsevier November 5, 2009

[6] An Iterative Algorithm For Trust Management And Adversary Detection For Delay Tolerant Networks Erman Ayday Faramarz Fekri IEEE Transactions on Mobile Computing (Volume:11 , Issue: 9)