A Survey on Efficient Detection of Selfish Nodes in MANET using A Collaborative Watchdog

P.S.Nandhini[1] N. Duraipandian[2]
[1]P.G. Scholar [2]Professor
[1,2]Department of Computer Science & Engineering
[1,2]Velammal Engineering College, Chennai, India

Abstract— Misbehavior of Nodes is basically due to selfish or faulty nodes or malicious reasons can degrade the performance of Mobile ad-hoc networks (MANETs). To handle with misbehaviour in such self-organised networks, nodes need to adapt their strategy to changing levels of cooperation. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behaviour. Hence, the overall network performance could be affected seriously. The well-known mechanism to detect selfish nodes are watchdogs. However, the detection process handled by watchdogs can fail, reporting false positives and false negatives which leads to wrong operations. Besides, depending on local watchdogs alone can lead to bad performance when detecting selfish nodes, in term of precision and speed.. Thus, we propose 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. 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).

Key words: Wireless Networks, MANETS, Cooperation, Selfish Nodes, Performance Evaluation

I. INTRODUCTION

The cooperative operation and self-organizing of mobile and wireless nodes within ad-hoc networks bears several research challenges, of which routing is prominent. Currently, cooperative networking is receiving attention as an emerging network design strategy for future mobile wireless networks. The cooperation on the networks is generally contact-based. Mobile nodes can directly communicate with each other, if they are in the communication range (that is, if the contact occurs).Thus, nodes could have a selfish behaviour, unwilling to forward packets to others. Selfishness means some nodes refuse to forward packets to save their own resources.

We, consider that watchdogs are the appropriate mechanism to detect these situations. Essentially, watchdog systems overhear wireless traffic and analyse it to decide if neighbouring nodes are not cooperating. Several works have studied the impact of node selfishness on MANETS proposing different detection mechanisms [2]-[5].The rest of the paper is organised as follows

- Section 2: Classification of Node Misbehavior
- Section 3: Detection and Reputation System
- Section 4: The Collaborative Watchdog
- Section 5: Use of Second-hand Information
- Section 6: Performance Evaluation.

II. CLASSIFICATION OF NODE MISBEHAVIOR

There is no common classification of node misbehaviour. The authors of [4] and related studies have their own categories of classification of misbehaving nodes. Since these categories and especially the accuracy of their definition do not suit analytical modes, we need to classify misbehaviour differently. From a technical perspective, these degrees of freedom may be implemented as follows:

- Time, the on/off behavior of a node may be characterized using {start time, stop time}.
- Degree of behavior, giving the probability with which the node behaves as specified {p}.
- Plane of behavior, controlling which part of the protocol is affected {control plane, data plane, both}.
- Type of behavior, determining which action to perform {forward packet, discard packet, inject packet}.
- Behavior against whom, which nodes are affected from the behavior {all nodes, a subset of nodes, a superset of nodes, none}.

We, additionally characterized node misbehaviour using some well- defined classes to follow further analytically study. Here is a non-exhaustive list of the derived classes:

- Cooperative nodes, which comply to the standard, at all times.
- Inactive nodes, which include lazy nodes (unintentionally misconfigured) and constrained nodes (e.g. energy-constraint or field-strength-constraint).
- Selfish nodes, which optimize their own gain, with neglect for the welfare of other nodes.
- Malicious nodes, which inject false information and/or remove packets from the network. We note that, depending on the degree of non-cooperation the nodes exhibit, selfishness may partially overlap with inactivity.

A. Inactive Nodes

The behavior of *inactive nodes* can be easily described and traced analytically. In reality, they may be constrained nodes or lazy and misconfigured nodes which are intentionally or unintentionally not actively participating in route discovery and packet forwarding.

1) Definition:

An *inactive node* is neither active on the control plane nor on the data plane. It does not cooperate during the routing process and does not forward any packets.

B. Selfish Nodes

Selfish nodes maximize their own gain. They do not aid other nodes on the data-plane, thus actively discarding packets routed through them. On the other hand, to be able to send and receive packets from other nodes. They are cooperative on the control-plane, namely the routing process.

1) Definition:

A selfish node does not forward any data packets for other nodes except for himself. He cooperates during the route discovery cycle to maintain a concise routing table and to be present in other routing tables.

C. Malicious Nodes

Malicious nodes reduce the utility of the network, without regard for their own gain. Maliciousness may naturally take on many forms. We choose the notion of black holes, which masquerade with a fake destination and thus try to attract routes and data packets.

1) Definition:

A malicious node abuses the cooperation among nodes to hinder operation of the network.

III. Detection and Reputation System

The goal of a detection and reputation system is to enable nodes to adapt to changes in the network environment caused by misbehaving nodes by the following functions.

A. Monitoring:

The goal of monitoring is to gather first-hand information about the behavior of nodes in the network. Monitoring systems detect misbehavior that can be distinguished from regular behavior by observation. Not forwarding is just one of the possible types of misbehaviour in mobile ad-hoc networks. Several others, mostly concerned with routing rather that forwarding have been suggested, such as black hole routing, gray hole routing, warm hole routing. We classify misbehavior types as packet dropping, modification, fabrication, or timing misbehavior; many of these can be detected by direct observation as we have shown in a test-bed implementation [5]. To detect misbehavior, nodes take into account the packets they receive (e.g. a received acknowledgment from the destination means that all the nodes on the route cooperated in forwarding) and they can also use enhanced passive acknowledgments (PACK) by overhearing the transmissions of the next hop on the route, since they are within range when using omnidirectional antennas. For instance, if they do not overhear a retransmission to the following node within a timeout of e.g. 100 ms or if the overheard transmission shows that the packet header has been illegitimately modified, they conclude misbehavior. To distinguish from physical failures of the next hop, the timeout allows for retransmission attempts if the transmission of the next hop fails. If there are link failures over a longer time, the node can expect a route error (RERR). To account for connectivity problems at the monitoring node itself, it disregards PACK time outs in the case of link-layer error messages received from its own interface. In addition to a list of known types of misbehavior, nodes can automatically learn about new misbehavior in analogy to the human immune system [1].

B. Reputation:

Reputation systems are used for example in some on-line auctioning systems. They provide a means of obtaining a quality rating of participants of transactions by having the buyer and seller give each other feedback. The two main ideas behind reputation systems are that, first, it is used to serve as an incentive for good behavior to avoid the negative consequences a bad reputation can entail. Second, it provides a basis for the choice of prospective transaction partners. The relevant properties of a reputation system are discussed in the next sections.

The terms reputation and trust have been used for various concepts, also synonymously. Wedefine *reputation* here to mean the performance of a node in participating in the base protocol as seen by others. For mobile ad-hoc networking this means participation in routing and forwarding. By *trust* we denote the performance of a node in the policing protocol that protects the base protocol, here the reliability as a witness to provide honest reports. The use of second-hand information, i.e. reputation information obtained from others, enables nodes to find out about misbehaving nodes before making a bad experience. Also, in mobile ad-hoc networks, nodes might not meet every node that they need for multi-2 hop forwarding, but with second-hand information they can make informed decisions about which nodes to use for their paths.

C. Response:

Detection and reputation systems aim at isolating nodes that are deemed misbehaving by not using them for routing and forwarding, and most also isolate them additionally by denying them service. This isolation has three purposes. The first is to reduce the effect of misbehavior by depriving the misbehaving node of the opportunity to participate in the network. The second is to serve as an incentive to behave well to not be denied service. Finally, the third is to obtain better service by not using misbehaving nodes on the path. The isolation is done by each node autonomously, without consensus or human intervention. Monitoring, reputation, and response come at the price of overhearing transmissions of others, keeping a reputation rating about nodes of interest and updating it at each observation. The gain can be measured in increased throughput and decreased number of lost packets, i.e. needless transmissions [2]. Note that the cost, in terms of battery use, of transmissions is much higher than that of simple computations. Nodes have to listen to traffic anyway to find out whether it is for them.

IV. A Collaborative Watchdog

A way to reduce the detection time of selfish (or non-cooperative) nodes in a network is the collaborative watchdog. Although some of the aforementioned paper [5] introduced some degree of collaboration on their watchdog schemes, the diffusion was very costly (usually based on sending periodic messages).

This paper introduces an efficient approach to reduce the detection time of selfish nodes based on contact dissemination. If one node has previously detected a selfish node using its watchdog it can spread this information to other nodes when a contact occurs(that is, with the use of second hand information). We say that a node has a *positive* if it knows the selfish node. The detection of contacts

between nodes is straightforward using the node's watchdog. Notice that the watchdog is overhearing the packets of the neighbourhood; thus, when it starts receiving packets from a new node it is assumed to be a new contact. Then, the node transmits one message including all known positives it knows to this new contacted node.

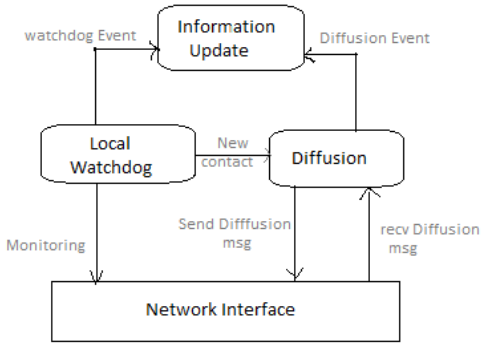

Fig 1: CoCoWa Architecture

The number of messages needed for this task is the overhead of the collaborative watchdog. Formally, we have a network of N wireless mobile nodes, with C collaborative nodes and S selfish nodes. Initially, the collaborative nodes have no information about the selfish nodes. A collaborative node can have a positive when a contact occurs in the following way:

A. *Selfish Contact:*

If one of the nodes is the selfish node. Then, the collaborative node *can* detect it using its watchdog and have a positive about this selfish node. Nevertheless, a contact does not always imply a detection. To model this fact, we introduce a probability of detection (p). This probability depends on the effectiveness of the watchdog and the type of contact (for example if the contact time is very low, the watchdog does not have enough information to evaluate if the node is selfish or not).

B. *Collaborative Contact:*

Both nodes are collaborative. Then, if one of them has one or more positives, it can transmit this information to the other node; so, from that moment, both nodes have these positives. As in the selfish contact case, a contact does not always imply a collaboration. We model this with the probability of collaboration (p). The degree of collaboration is a global parameter of the network to be evaluated. This value is used to reflect that either a message with the information about the selfish nodes is lost or that a node temporally does not collaborate (for example, due to a failure or simply because it is switched off). In real networks, full collaboration (pcc=1) is almost impossible.

Although defining a reaction scheme is out of the scope of this paper, there are basically two approaches in the literature: isolation and incentivation. Isolation methods are intended to keep the misbehaving nodes outside the network, excluding them from all kinds of communication. Incentivation methods try to convince the selfish nodes to change their behaviour, and become collaborative instead of selfish, using a virtual payment scheme or a similar mechanism.

V. USE OF SECOND HAND INFORMATION

In the scenario from fig-1, since A is not in range with C, it cannot directly observe its behavior and thus cannot detect C's misbehavior. This is solved by allowing the use of second-hand information. In CONFIDANT, short for Cooperation of Nodes, Fairness In Dynamic Ad-hoc Networks, in addition to keeping track of direct local observation, nodes publish, as shown in Figure 1(b), their first-hand information from time to time by local broadcasts to exchange information with other nodes. The published information from others is called second-hand information. It is not propagated further. Nodes rely mostly on local information but they can also take into account the local information of other nodes to gradually get a global view of the network. A thus receives information from its neighbors, here E, F, G, and B, about other nodes, including C. Again, since A has no first-hand information about C in our scenario, it can only find out about C's misbehavior by second-hand information. There is, however, a problem since second-hand information can be spurious, e.g. false accusations. There is a trade-off between the detection speed gained by second-hand information (detection before encounter) and the classification vulnerability introduced.

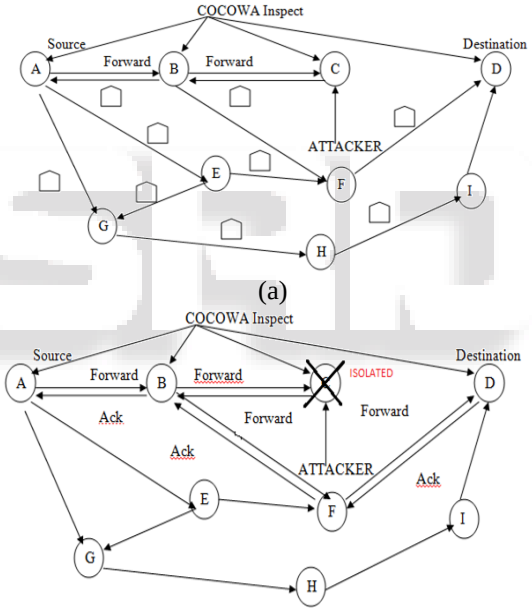

Fig. 2: Second-hand Information

In the above Fig-2(a), the source node A sends the data to the destination node D through the nodes which falls in its communication range. Here, the node C acts as a selfish node which resists forwarding the node further. Thus, the second hand information is passed to all the other nodes in the network.

In the fig-2(b),by the use of second-hand information the node C is been isolated and the data is sent through A-B-F-D. Finally, the data is been forwarded to the destination node.

VI. PERFORMANCE EVALUATION

To evaluate the performance of the CoCoWa, we use the ns2 discrete event simulator. To measure the minimum detection time for detecting the selfish nodes, we measure the amount

of time consumption of each node through the trace graph results after running the simulation as per the scenario.

A Graph is plotted with Detection Time along X-Axis and Nodes along Y-Axis to determine the efficient detection of the selfish nodes in minimal time consumption. Initially, general watchdog is found to consume maximum amount of time to detect the selfish nodes considering the false positives and false negatives. Further, CoCoWa consumes less energy in comparison with a general watchdog.

Therefore, CoCoWa is can detect the selfish nodes more effectively considering false positives, false negatives and malicious nodes in minimal detection time.

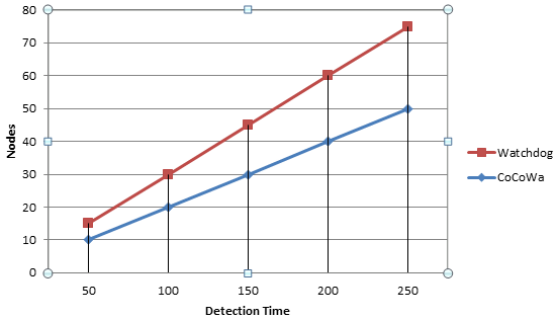

Fig. 3: Performance Evaluation: CoCoWa Vs Watchdog

VII. Conclusion

Thus, CoCoWa improve the effectiveness of detecting selfish nodes by reducing the harmful effect of false negatives, false positives and malicious node. Analytical and experimental results show COCOWA can reduce the overall detection time, with a reduced overhead. Thus using COCOWA, the effect of malicious or collosive nodes are reduced by using the Second-Hand information which is send to all the collaborative nodes in the network.

References

[1] S. Abbas, 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.

[2] S. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hocnetworks by reputation systems," IEEE Commun. Mag., vol. 43,no. 7, pp. 101–107, Jul. 2005.

[3] A. Chaintreau, P. Hui, J. Crowcroft, 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.

[4] S. Eidenbenz, G. Resta, and P. Santi, "The COMMIT protocolfor 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.

[5] E. Hern-andez-Orallo, 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.

[6] M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz, "On the effect of node misbehavior in ad hoc networks," in Proc. IEEE Int. Conf. Commun., 2004, pp. 3759–3763. Internet Syst., 2010, pp. 543–552.

[7] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in Proc. Int. Conf. Commun. Workshop, 2010, pp. 1–5.

[8] M. Karaliopoulos, "Assessing the vulnerability of DTN data relaying schemes to node selfishness," IEEE Commun. Lett., vol. 13, no. 12, pp. 923–925, Dec. 2009.

[9] Y. Li, G. Su, D. Wu, D. Jin, L. Su, and L. Zeng, "The impact of node selfishness on multicasting in delay tolerant networks," IEEE Trans. Veh. Technol., vol. 60, no. 5, pp. 2224–2238, Jun. 2011.

[10] K. Paul and D. Westhoff, "Context aware detection of selfish nodes in DSR based ad-hoc networks," in Proc. IEEE Global Telecommun. Conf., 2002, pp. 178–182.

[11] C. K. N. Shailender Gupta and C. Singla, "Impact of selfish node concentration in MANETs," Int. J. Wireless Mobile Netw., vol. 3, no. 2, pp. 29–37, Apr. 2011.

[12] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mobile Comput., vol. PP, no. 99, 2012, http://doi.ieeecomputersociety.org/10.1109/TMC.2012.257

