

A Survey on Collaborative contact-based Selfish node detection in Mobile ad hoc Network

M.MADHUMATHI, S. Sindhuja
Department of Computer Science & Engineering,
SNS College of Engineering,
Coimbatore, INDIA.

Abstract- Mobile ad-hoc networks (MANETs) depends on network cooperation schemes to work properly. It assume that mobile nodes voluntary cooperate in order to work properly. Nevertheless, if nodes have a selfish behaviour and are unwilling to cooperate, the overall network performance could be seriously degraded. The use of watchdogs is a well-known mechanism to detect selfish nodes. Sometimes watchdogs can fail, generating false positives and false negatives that can induce to wrong operations. In this paper we propose a collaborative contact-based watchdog approach, which is based on the fast diffusion of selfish nodes awareness when a contact occurs. Then, we introduce an analytical model to evaluate the time of detection and the overhead of our collaborative watchdog approach for detecting selfish nodes.

Index Terms—Wireless networks, MANET, selfish nodes, 4D-CTMC

I.INTRODUCTION

Mobile ad hoc networks are widely used and they are infrastructure less. It can be installed without any base station and dedicated routers. The networks of mobile nodes are connected by wireless links without using any pre-existent infrastructure. Each node is free to move independently in any directions and can directly communicate with each other if a contact occurs.

In MANETs, nodes rely on network cooperation schemes to work properly. The more nodes they co-operate can able to send the packets more easily. But supporting a MANET is a cost-intensive activity for a mobile node. Detecting routes and forwarding packets consumes more local CPU time, memory, network-bandwidth, and last but not

least energy. Therefore there is a very strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data. A node may behave selfishly by agreeing to forward the packets and then failing to do so, in order to save its own resource. Nevertheless, in the real world, most nodes have a selfish behavior and are unwilling to forward packets for others. Additionally, network performance could be drastically reduced. To this end, an effective protection against misbehaved nodes will be mandatorily important to preserve the correct functionality of the MANET.

There are two approaches in dealing with selfish nodes. The first approach tries to give a motivation or incentive based approach for participating in the network function. A typical system representing this approach is Nuglets. The authors suggest to introduce a virtual currency called Nuglets that is earned by relaying foreign traffic and spent by sending own traffic. Most of the existing work in this field concentrates on the second approach: Detection and exclusion. The first to propose a solution to the problem of selfish (or as they call it "misbehaving") nodes in an ad hoc network

The main intention of a Selfish node attack is to preserve its own resources, e.g. battery life or its bandwidth. Selfish nodes behave adversely by receiving and forwarding packets of its interest and it may discard packets that are of no interest to conserve energy. Therefore, it may either drop data packets or refuse to retransmit routing packets that are not concerned to it. Some of the properties of selfish nodes are, not participating in the process and progress of routing, and not sending reply message.

Intentionally uncooperative behavior (misbehavior) may result in a total communication breakdown. Additionally, some nodes can exhibit malicious behavior. The effect of colluding or

malicious nodes can even be more harmful, since these nodes trying to disturb the normal network behaviours. Malicious nodes are very hard to detect using watchdog mechanism, as they can intentionally participate in the network communication having the only goal to hide their behavior from the network.

Thus detecting such selfish and malicious nodes quickly and accurately is important to increase the overall performance of the network.

Our paper introduces an efficient approach as Collaborative contact-based watchdog (CoCoWa) to reduce the detection time of selfish nodes based on contact dissemination. If one node has earlier detected a selfish node using its watchdog it can spread this information to other nodes whenever a contact occurs. If a node identifies a selfish node, then that node diffuses that information to all the other nodes. Whenever watchdog overhears new packets from a node, it is assumed to be a new node and it disseminates that information to all the other nodes. Then, the node transmits only one message including all known positives it knows to this new contacted node.

Then, we introduce an analytical model Continuous Time Markov Chain (CTMC) to evaluate the detection time and the cost of this collaborative approach

II. LITERATURE REVIEW

1. Credit Based Schemes

The simple idea of credit-based schemes is to provide motivations for nodes to faithfully perform networking functions. So as to achieve this goal, virtual currency or similar payment system may be set up. Each node is paid for providing services to other nodes. When they request from other nodes to help them for forwarding the packets, they use the same payment system to compensation for such services. Credit based schemes can be implemented using two models:

1. The Packet Purse Model (PPM) and Packet
2. Trade Model (PTM)

1.1. The Packet Purse Model:

In this model, the originator of the packet will pay for the packet forwarding service for which a node is forwarding the packets. Then the service charge is distributed among the forwarding nodes. The originator will load it with the number of sufficient beans to reach the required destination. Each forwarding node gains one or several beans from the packet and thus, increases the stock of its beans. If the packet does not have sufficient beans to be forwarded means, then that packet will be

discarded. The main basic problem with this approach is that, it might be difficult to guess the number of beans that are required to reach a given destination.

1.2. The Packet Trade Model:

In the packet trade model, the packet does not carry any beans but it is traded for beans by intermediate nodes. Each intermediate node buys the beans from its previous one for some beans and sells it to the next node for more beans. The overall cost of forwarding the packet is covered by destination of the packet. An advantage of this method is that the originator does not have to know in earlier the number of beans required to deliver a packet.

The drawback of this packet trade model is that, it needs tamper-proof hardware. This hardware is essential at each node to prevent the node from illicitly increasing its own nuglets and also to ensure that the correct amount of nuglets are deducted or credited at each node.

2. Sprite:

Sprite: A Simple, Cheat-proof, Credit-based system for mobile ad hoc networks, in this method before sending the message to the intermediate node source node should sign it and the intermediate node should verify it. AC verifies that the signature are correct and then guarantee that the payment is correct. It does not need any tamper proof hardware; it mainly focuses on node selfishness. Whenever a node receives a message, it keeps a receipt of that message. It uses this credit to provide motivation to selfish nodes. There is a credit clearance system that controls the credit of each node that relay messages more successfully. Depending upon the receipt submitted, CCS fixes charge and credit to each node. With respects to prevent the denial-of-service attack on the destination node, the sender is charged, by sending it a large amount of traffic.

The main drawback of sprite is that it charges only the source node and it generates receipt for every message that causes overhead.

3. Reputation-Based Systems:

In reputation based schemes, the network nodes together will detect and affirm the misbehavior of a suspicious node. Such assertion is then propagated throughout the network, so that the misbehaving node will be discontinued from the rest

of the network. There are two models in reputation based schemes as:

1. Watchdog Model
2. Pathrater

3.1. Watchdog:

Each and every node maintains a buffer of recently sent packets and compares each overheard packet with the packet in the buffer to observe if there is any match. If there is any match, then that packet in the buffer is removed and elapsed by their watchdog, since it has been forwarded on. If a packet has remained in the buffer for a longer time than a certain period, the watchdog increments a failure count for the nodes that are responsible for forwarding on the packet. If the count exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source to notify that the node is a misbehaving node. To illustrate how the watchdog works. Consider suppose there exists a path from node S to D through intermediate nodes A, B, and C. Node A cannot transmit all the way to node C, but it can listen in on node B's traffic. Thus, when A transmits a packet for B to forward to C, A can often tell if B transmits the packet.

The problem with watchdog method is that, it might not detect any misbehaving node in the presence of

- 1) Ambiguous collisions
- 2) Receiver collisions
- 3) limited transmission power
- 4) false misbehavior
- 5) Conclusion and
- 6) partial dropping.

3.2. Pathrater:

The pathrater, which has been run by each node in the network, combines the knowledge of misbehaving nodes with the link reliability data to pickup the routes that are most likely to be consistent. Each node maintains a ranking for every other node it knows regarding in the network. It calculates the path metric by averaging the node ratings in the path. If there are multiple paths to the same target, then the path with the highest metric is selected.

4. CONFIDANT:

CONFIDANT aims at detecting and isolating unhelpful nodes. When any misbehavior is detected, then the monitoring nodes will broadcast alarm messages to the nodes in order to notify their peers of the detected misbehavior and alter the corresponding reputation values.

In CONFIDANT, each node has four components:

- a monitor
- a trust manager
- a reputation system and
- path manager

These four components interact with each other to provide and process protocol information.

Monitor:

The monitor is the corresponding to the neighbour watchdog, where nodes locally monitor the deviating behavior of nodes. The monitor reports if any suspicious events occurrences and any incoming ALARM messages to the trust manager.

Trust manager:

The trust manager will makes decisions about providing or accepting route information, after then only it will start accept a node as part of a route or taking part in a route originated by another node.

Reputation system:

The reputation system has a protocol that manages a table consisting of entry for nodes and along with their rating. The rating will be changed only when there are sufficient confirmations of malicious behaviour.

Path manager:

The path manager will performs the following functions as: path re-ranking will be done according to reputation value of the nodes in their path; deletion of paths will happen when there are any malicious nodes, then action on getting a request for a route from a malicious node (e.g. ignore, do not send any reply) and atleast the action on getting request for a route containing a malicious node in the source route.

The drawback of CONFIDENT protocol is node authentication is not checked, that is it assumes that nodes are authenticated, but a compromised node can send false ALARM messages. Another one is that each node monitor the behaviour of its next hop neighbors in a similar manner to watchdog. Deciding the criteria for maintaining the friends list by Trust Manager is difficult.

5. OCEAN:

Bansal and Baker also suggested a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) which is an extension of the DSR protocol. OCEAN like the previous methods uses a monitoring plus a reputation system. However, conflicting to previous approaches, OCEAN depends only on its own observation in order to avoid the new vulnerability of false allegation from second-hand reputation exchanges. So, OCEAN can be depicted a stand-alone architecture.

OCEAN has classified routing misbehavior into two classes: misleading and selfish. If a node takes part in the route discovery but does not forward a packet, then its class is identified as misleading and

it also misleads other nodes to route packets through it. But if a node does not participate in the route discovery, then it is considered to be selfish. In order to identify the misleading routing behaviors, a node should buffers those packet checksum after forwarding a packet to a neighbor. Then it starts monitoring whether the neighbor attempts to forward the packet within a given time. As a result of monitoring the nodes, either a negative or positive event is created to update the neighbor rating. In adding to it that all the traffic from the misbehaving neighbor node will be rejected. This node is given an explicit time to return to the network because it is likely that it is wrongly suspect of misbehaving or if it is a misbehaving one in the sense, it must be enhanced in this time period. Each node has a mechanism of preserving chip counts for each of their neighbor in order to discover the selfish behavior. The neighbor node will increase chips count when accelerating a packet for other nodes and reducing the chips count when requesting others nodes to forward a packet. If the chip count of the neighbor node is under the threshold, then the packets coming from that neighbor node will be rejected.

The advantages of OCEAN technique is that it will distinguish the selfish node and the misleading nodes, it maintains overall network throughput with the presence of selfish nodes at network layer. But it fails to punish those misbehaving nodes severely.

6. Standard Watchdog:

The standard watchdog first overhears that how many packets has been transmitted and how many packets has been received by its neighbor nodes. Then it starts counting that how many packets should be retransmitted, then it computes a trust level for each and every neighbor nodes as the ratio of "packets retransmitted to the number of packets that should have been retransmitted". If a node retransmits all the packets then it has a trust level of 1. If a node has a trust level that is lower than that of the configured tolerance means, then that node is identified as malicious.

The disadvantage of this protocol is that it will decrease the network performance and it does not support high number of nodes. Another drawback is that it doesn't detect the actual reason for the packet loss.

7. Bayesian Watchdog:

The Bayesian Watchdog has been established in order to overcome the problems in standard watchdog. Bayesian watchdog is a tool that merges both the watchdog mechanism and the Bayesian filters. It is more robust against environmental noise but consume more CPU resources. The advantage of

the Watchdog protocol is that, they make use of only local information and are proficient to spot the malicious node. Watchdog protocol which acts as a good intrusion detection mechanism in the network. In order to overcome the disadvantages of the Watchdog protocol, the Bayesian Watchdog mechanism has been introduced in which it perfectly differentiate the packet loss due to congestion and the packet loss due to the presence of a malicious node in the network.

8. Collaborative Watchdog:

The collaborative watchdog mechanism is used to reduce the detection time of selfish nodes based on contact dissemination. If one node has formerly detected a selfish node using its watchdog it can spread that information to other nodes. We say that a node has a positive if it knows the selfish node. When the watchdog is overhearing the packets of the neighborhood, hence, it starts acceptance packets from a new node it is assumed to be a new contact. Then, the node transmits only one message including all the known positives to their neighbor node. The number of messages needed to perform this task is the overhead of the collaborative watchdog

The drawback of this method is that the diffusion is costly since they are based on periodic message dissemination

CONCLUSION AND FUTURE WORK

One of the problems in MANET is the presence of selfish nodes in the network, which could seriously degrade the network performance. So we introduced a CoCoWa as a collaborative contact-based Watchdog mechanism in order to overcome the drawbacks from previous approach. The introduced technique will reduce the time for the detecting selfish nodes. The working of the cocowa is based on the diffusion of its known positive detection and negative detections. Whenever a contact occurs between any two collaborative nodes, the diffusion module transmits its known positive and negative detections to the neighbor nodes. The analytical and experimental results shows that cocowa model have highly reduced the overall selfish node detection time with a reduced overhead as message cost. Finally, using CoCoWa we can reduce the effect of malicious or collusive nodes. If however malicious nodes spread false negatives or false positives in the network means, then in that situation CoCoWa model is able to reduce the effect of these malicious nodes quickly and effectively. The future work includes the use of cluster-based selfish node identification with encounter algorithm through this; we can even reduce

the detection time of selfish node along with reduced overhead and increased throughput.

REFERENCES:

- [1] S. Buchegger and J.Y. Le Boudec, "Self-Policing mobile ad hoc networks by reputation Systems," *IEEE Commun. Mag.*, vol. 43, no. 7, pp. 101–107, Jul. 2005.
- [2] L. Buttyan and J.P. Hubaux, "Enforcing Service availability in mobile ad-hoc WANS," In Proc 1st Annu Workshop Mobile Ad Hoc Netw Comput. 2000, pp. 87–96.
- [3] L. Buttyan and J.P. Hubaux, "Stimulating Cooperation in self-organizing mobile ad hoc Networks," *Mobile Netw Appl.*, vol. 8, pp. 579–592, 2003.
- [4] S. Eidenbenz, 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.
- [5] E. Hernandez 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] E. Hernandez-Orallo, M. D. Serrat Olmos, J. C. Cano, C. T. Calafate, and P. Manzoni, "Evaluation of collaborative Selfish node Detection in MANETS and DTNs," in Proc 15th ACM Int. Conf. Modeling, Anal. Simul Wireless Mobile Syst., New York, NY, USA, 2012, pp. 159–166.
- [7] M. Hollick, J. Schmitt, C. Seipl, and "On the Effect of node misbehavior in ad hoc Networks," in Proc IEEE Int Conf Commun, 2004, pp. 3759–3763.
- [8] 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.
- [9] F. Kargl, A. Klenk, S. Schlott, and M. Weber, "Advanced detection of selfish or malicious Nodes in ad hoc networks," in Proc. 1st Eur. Conf. Security Ad Hoc Sens. Netw 2004, pp. 152–165.
- [9] F. Kargl, A. Klenk, M. Weber, and S. Schlott, "Sensors for detection of misbehaving nodes in MANETs," in Proc. Detection Intrusions Malware Vulnerability Assessment, 2004, pp 83–97.
- [10] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation mechanism to Enforce node cooperation in mobile ad hoc Networks," in Proc. 6th Joint Working Conf Commun Multimedia Secure, 2002, pp. 107–121.
- [11] 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.
- [12] M. D. Serrat-Olmos, E. Hernandez-Orallo, J.-C. Cano, C.T. Calafate, and P. Manzoni, "A Collaborative Bayesian watchdog for Detecting black holes in MANETs," in Proc 6th Int.Symp Intel Distribute. Comput VI, 2012, vol. 446, pp. 221–230.
- [13] C. K. N. Shailender Gupta and C. Singla, "Impact of selfish node concentration in MANETs," *Int. J. Wirelss Mobile Netw.*, vol 3, no. 2, pp. 29–37, Apr. 2011.
- [14] Toh, D. Kim, S. Oh, and H. Yoo, "The Controversy of Selfish nodes in ad hoc Networks," in Proc Adv Commun Technol., Feb. 2010, vol. 2, pp. 1087–1092.
- [15] Y. Yoo, S. Ahn, and D. Agrawal, "A credit-Payment scheme for packet forwarding Fairness in mobile ad hoc networks," in Proc IEEE Int. Conf Commun. May 2005, vol. 5, pp. 3005–3009.

AUTHORS:



Madhumathi.Mss received B.E degree in computer science and Engineering from Sri Shakthi institute of Engineering & Technology, Coimbatore. She is currently pursuing her ME degree in SNS College of Engineering, Coimbatore. Her Research interests include Security in MANETS.