ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Detection of Selfish Nodes with the Help of a Collaborative Contact-Based Watchdog

Kondru Mounika
M.Tech Student
Department of CSE,
ASR College of Engineering,
(Affiliated to JNTUK, Kakinada)
Tetali, Tanuku,
West Godavari Dt, Andhra Pradesh.

J.Rajakala
Associate Professor,
Department of CSE,
ASR College of Engineering,
(Affiliated to JNTUK, Kakinada)
Tetali, Tanuku
West Godavari Dt, Andhra Pradesh.

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***

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 behaviour (misbehaviour) may result in a total communication breakdown. Additionally, some nodes can exhibit malicious behaviour. 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 disemminate 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

LITERATURE REVIEW

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)

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.

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

correct amount of nuglets are deducted or credited at each node.

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 signs it and the intermediate node should verifies 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 measage, 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.

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

1. Watchdog Model
2. Pathrater

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 misbehaviour
5) Conclusion and
6) Partial dropping.

EXISTING SYSTEM:

The impact of node selfishness on MANETs has been studied in credit-payment scheme. In credit-payment scheme 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 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 reachability. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

DISADVANTAGES OF EXISTING SYSTEM:

- Increase the selfish nodes
- Increase the packet loss
- Reduce the throughput
- Increase overhead
- 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.

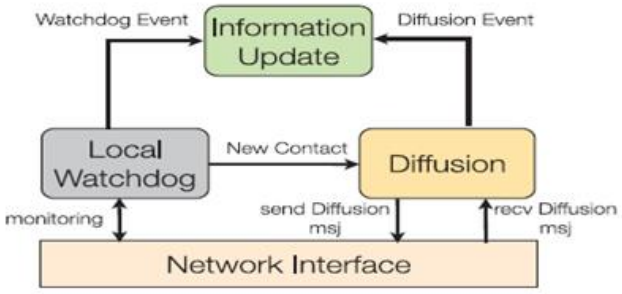
PROPOSED SYSTEM:

- This project 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. 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.

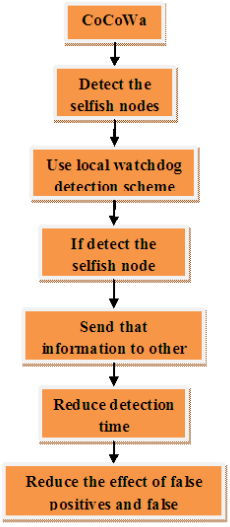
ADVANTAGES OF PROPOSED SYSTEM:

- Reduce the selfish nodes
- Increase the throughput
- Decrease the overhead

SYSTEM ARCHITECTURE:



BLOCK DIAGRAM:



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 indenification with encounter algorithm through this; we can even reduce the detection time of selfish node along with reduced overhead and increased throughput.

REFERENCES:

[1] Enrique Hern_andez-Orallo, Member, IEEE, Manuel David Serrat Olmos, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, Member, IEEE, "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 6, JUNE 2015.

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

[3]L. Butty_an 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.

[4]L. Buttyan and J.P. Hubaux, "Stimulating Cooperation in self-organizing mobile ad hoc Networks," Mobile Netw Appl., vol. 8,pp. 579– 592, 2003.

[5]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.

[6]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.

[7]E. Hern_andez- 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.

[8] M. Hollick, J. Schmitt, C. Seipl, and "On the Effect of node misbehavior in ad hoc Networks," in Proc IEEE Int ConfCommun, 2004, pp. 3759–3763.

[9]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.

[10]F. Kargl, A. Klenk, S. Schlott, and M. Weber, "Advanced detection of selfish or malicious Nodes in ad hoc networks,"in Proc. 1stEur. Conf. Security Ad Hoc Sens. Netw 2004, pp. 152–165.

[11]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.

[12]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.

[13]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.

[14]M. D. Serrat-Olmos, E. Hern_andez- Orallo, J.-C. Cano, C.T. Calafate, and P. Manzoni, "A Collaborative Bayesian watchdog for Detecting black holes in

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

MANETs," in Proc 6th Int.Symp Intel Distribute. Comput VI, 2012, vol. 446, pp. 221–230.

[15]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.

[16]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.

[17]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.