ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

Improving Selfish Node Detection In MANET Using A Collaborative Watchdog

R.Bhuvaneshwari[1],
M.E., Computer Science Student,
M.I.E.T Engineering College, Trichy,
bhuvanarkcse@gmail.com

G.Nalina Keerthana[2]
Assistant Professor, Department of CSE,
M.I.E.T Engineering College, Trichy
jjkgnk@gmail.com

A.Rachel Roselin[3]
M.E., Computer Science Student,
M.I.E.T Engineering College, Trichy
roseruby1993@gmail.com

***Abstract*—**Mobile ad-hoc networks (MANETs) assume that mobile nodes voluntary cooperate in order to work properly. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behaviour. Thus, the overall network performance could be seriously affected. The use of watchdog is a well-known mechanism to detect selfish nodes. However, the detection process performed by watchdogs can fail, generating false positives and false negatives that can induce to wrong operations. Moreover, relaying on local watchdogs alone can lead to poor performance when detecting selfish nodes, in term of precision and speed. This is especially important on networks with sporadic contacts, such as delay tolerant networks (DTNs), where sometimes watchdogs have lack of enough time or information to detect the selfish nodes. Thus, proposing collaborative contact-based watchdog (CoCoWa) as a collaborative approach based on the diffusion of local selfish nodes awareness whwn a contact occurs, so that information about selfish nodes is quickly propagated. This collaborative approach reduces the time and increases the precision when detecting selfish nodes.

Key words*—Selfish nodes,MANETs,CoCoWa,*Watchdog

I. INTRODUCTION

A set of autonomous wireless mobile nodes constructing a temporary network without the aid of a centralized infrastructure called MANET. Which communicate through multiple hops. The nature of MANET makes cooperation among the nodes essential for the system to be operational. Due to this fact, some nodes are not willing to forward packets to other misbehaving nodes. MANET is composed of mobile nodes without any pre-existent infrastructure and can be installed without any base station and dedicated routers. In MANETs, nodes act as both routers and end users. There are two types of MANETs: open and closed. In a closed MANET, all nodes will have a common goal and work towards that goal. In an open MANET, different nodes have different objectives. Data transmission is the most expensive function in the MANET compared to other functions. Misbehaving nodes are identified on the basis of packet dropped during the transmission of the next hop. When a node forward packets, proper transmission of packets by the next node is verified by watchdog. Misbehaviour is noticed, if that node refuses to transmit the packets. The misbehaving nodes can be identified in the level of connection as well as is forwarding level, Which is advantages of watchdog. The watchdog drawbacks are, False misbehaving, Minor dropping, Limited transmission power, Collision. There are two main strategies which help to deal with selfish behaviour: a) motivation or incentive based approaches, and b) detection and exclusion.

A wireless sensor network is an ad-hoc network which consists of large number of small inexpensive devices which are known as nodes. WSN consists of base station along with number of nodes that sense the environment and send data to the base station. The base station is more powerful than other nodes in terms of energy consumption and other parameters and serves as an interface to the outer world. When any node needs to send a message to the base station that is outside of its radio range, it sends it through internal nodes.

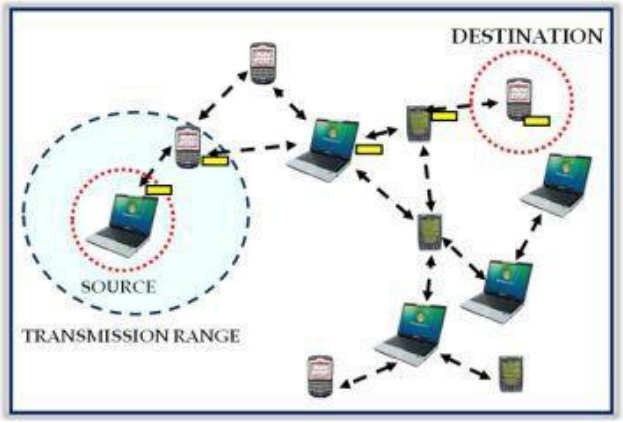

Fig. 1. MANET Architecture

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

A. Related Works

Reputation based technique depends on building a reputation metric for each node according to its behavioral pattern. A Watchdog is used by most of the systems as monitoring method to detect data packet non forwarding by overhearing the transmission of the next node. It is not only use same monitoring technique but also transmits the collected information to nearby nodes. Basically, Reputation is the amount of trust achieved by a member of a community in a specific domain of interest. Credit based technique incentives are provided on the basis how the networking functions are performed by a node. To achieve this goal, virtual currency or some kind of monetary system may be set up. Nodes are rewarded with incentives for providing services to other nodes. Even those nodes are paid who are requested for their services by the same payment system. There are two models used for implementation of Credit based schemes: The Packet Trade Model (PTM) and The Packet Purse Model (PPM). Christo Ananth et al. [6] discussed about a system,the effective incentive scheme is proposed to stimulate the forwarding cooperation of nodes in VANETs. In a coalitional game model, every relevant node cooperates in forwarding messages as required by the routing protocol. This scheme is extended with constrained storage space. A lightweight approach is also proposed to stimulate the cooperation.

All mechanisms mentioned above were put forward for detection and handling of misleading nodes.

B. Contributions

The procedure for CoCoWa optimization is the following: first, we need to obtain the network characteristics such as number of nodes, contact rate and degree of collaboration. These values can be experimentally measured or estimated. The performance of the local watchdog is also measured (or estimated), and it can depend on the network characteristics. Note that this local watchdog can be adjusted in terms of detection and precision. For example, in order to reduce the detection time in a network with a given contact rate and collaboration, the only solution is to increase the performance of the local watchdog module.

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. 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. Therefore, we consider that using an exponential fit is a valid assumption to model inter-contact times. Our analytical model assumes an exponential distributed inter-contact rate between nodes and, therefore, it is suited for modeling the contacts in MANETs and DTNs networks. This aspect is similar to the collaboration degree, but an increase of communication range of the malicious nodes will increase the information reception. The malicious nodes do not have information about all nodes; so, in order to send a positive/negative about a node, they must have contacted this node previously or have received a message from other nodes. In this case, the malicious node, in order to send wrong information, must know the state of each node. In other words it must have a perfect local watchdog.

II. SYSTEM MODEL

Nodes could have a selfish behavior, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources. 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 reach ability. 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.

A. Network Creation

The node name, internet protocol address, port number is get from the user. The path creation is dynamically created. The received data's is stored from the user successfully. The Nodes are loaded successfully for communication. The sensor nodes are randomly distributed in a sensing field. We are using mobile ad hoc network (MANET). This is the infra-structure-less network and a node can move independently. In a MANET, each node not only works as a host and also acts as a router. We can find the communication range for all nodes. Every node communicates only within the range. If suppose any node out of the range, node will not communicate those nodes or drop the packets. The network is modelled as a set of N wireless mobile nodes, with C collaborative nodes,M malicious nodes and S selfish nodes (N=C+M+ S). 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 overhead is the number of information messages transmitted up to the detection time.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

B. Diffusion Module

The diffusion module can generate indirect events when a contact with neighbour nodes occurs. Nevertheless, a contact does not always imply collaboration, so we model this probability of collaboration as pc. It is used to reflect that either a message with the information about the selfish node is lost, The Diffusion module has two functions: the transmission as well as the reception of positive (and negative) detections. A key issue of our approach is the diffusion of information. As the number of selfish nodes is low compared to the total number of nodes, positive detections can always be transmitted with a low overhead. However, transmitting only positive detections has a serious drawback: false positives can be spread over the network very fast. Thus, the transmission of negative detections is necessary to neutralize the effect of these false positives, producing excessive messaging or the fast diffusion of false negatives.

The information update module is driven by the previous local and indirect events. These events update the reputation about a node. The detection of selfish nodes and the detection of new contacts. The local watchdog can generate the following events about neighbor nodes: PosEvt (positive event) when the watchdog detects a selfish node, NegEvt (negative event) when the watchdog detects that a node is not selfish, and NoDetEvt (no detection event) when the watchdog does not have enough information about a node. The detection of new contacts is based on neighbourhood packet overhearing; thus, when the watchdog overhears packets from a new node it is assumed to be a new contact.

D. Malicious Node And Attacker Model Detection

Malicious nodes attempt to attack the CoCoWa system by generating wrong information about the nodes. Thus, the attacker model addresses the behaviour or capabilities of these malicious nodes. A malicious node attack consists of trying to send a positive about a node that is not a selfish

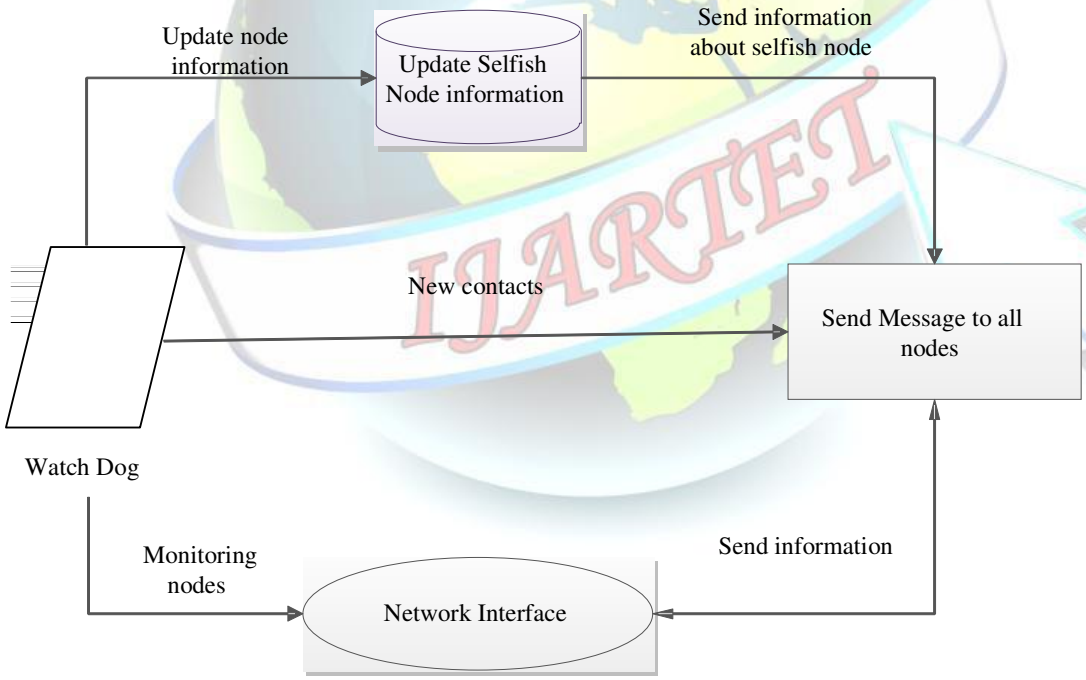

Fig. 2. System Architecture

C. Information update

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

node, or a negative about a selfish node, with the goal of producing false positives and false negatives on the rest of nodes. In order to do this, it must have some knowledge about the way CoCoWa works.

III. PERFORMANCE EVALUATION

System Implementation is the stage in the project where the theoretical design is turned into a working system. The most critical stage is achieving a successful system and in giving confidence on the new system for the user that it will work efficiently and effectively. The existing system was long time process. which has a menu-based interface, graphical interface for the end user. After coding and testing, the project is to be installed on the necessary system. The executable file is to be created and loaded in the system. The performance of the local watchdog is also measured, and it can depend on the network characteristics. Note that this local watchdog can be adjusted in terms of detection and precision. usually, the greater the precision, the lesser the detection ratio, as the local watchdog needs more packet overhearing to generate a more precise detection.

IV. CONCLUSION

This paper proposes 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 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 issued, with a reduced overhead. Finally, using CoCoWa we can reduce the effect of malicious or collusive nodes. If malicious nodes spread false negatives or false positives in the network CoCoWa is able to reduce the effect of these malicious nodes quickly and effectively. In short, the combined effect of collaboration and reputation of our approach can reduce the detection time while increasing the global accuracy using a moderate local precision watchdog.

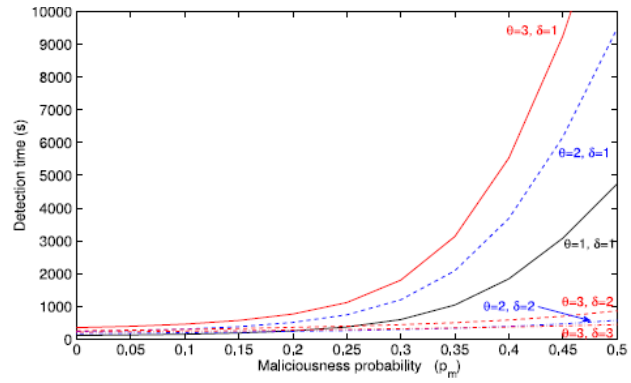

Fig. 3. Detection Time Of Selfish Node

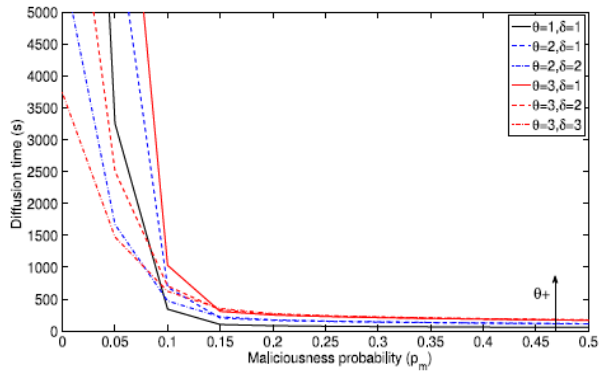

Fig. 4. Diffusion Time Of False Positive

V. FUTURE ENHANCEMENT

In this work we find the selfish node behaviour in mobile ad-hoc network, using collaborative contact based watchdog methods. Additionally, we have shown that CoCoWa is also effective in opportunistic networks and DTNs, where contacts are sporadic and have short durations, and where the effectiveness of using only local watchdogs can be very limited. In future we are going to avoid energy loss which consider data loss we going to consider RMER algorithm.

REFERENCES

[1] Ateniese G., Fu K., Green M. and Hohenberger S. (2005), 'Self-Policing Mobile ad hoc network by reputation system', IEEE Commun. Mag., vol. 43, no. 7, pp. 101-107.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

[2] Bansal S., and Baker M. (2003), 'Observation-based cooperation enforcement in ad hoc networks'.

[3] Buttyan L. and Hubaux J.-P. (2008), 'Enforcing Service availability in mobile ad-hoc WAN_s', in Proc. 1st Annu. Workshop Mobile Ad Hoc Netw. Comput., pp. 87-96

[4] Buttyan L., and Hubaux J.-P. (2003), 'Stimulating co-operation in self- organizing mobile ad hoc networks', in Mobile Network Application., vol. 8, pp. 579-592.

[5] Chaintreau A., Hui P., Diot C. and Scott J. (2007) , 'Impact of human mobility on opportunistic forwarding algorithms', in Mobile Computing, vol. 6. pp. 606-620.

[6] Christo Ananth, M.Muthamil Jothi, A.Nancy, V.Manjula, R.Muthu Veni, S.Kavya, "Efficient message forwarding in MANETs", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE),Volume 1,Issue 1,August 2015,pp:6-9.

[7] Hollick M., Schmitt J. and Seipl C. (2004), 'On the effect of node misbehavior in ad hoc networks', in Conf.Communication, pp. 3759-3763.

[8] Kargl F., Klenk A. and Weber M. (2004), 'Advanced detection of selfish or malicious nodes in ad hoc networks', in Conf.Security Ad-Hoc Sensor Network, pp. 152-165.

[9] Zhang Y., Lee W. and Huang Y.-A. (2003), 'Intrusion detection techniques for mobile wireless networks', in Wireless Network, vol.9., pp. 545-556.

AUTHORS

R.Bhuvaneshwari, She has received B.E Computer science and Engineering degree from Mount Zion college of engineering and technology, Pudukkottai in 2014 and currently pursing ME Computer science and Engineering degree in M.I.E.T engineering college, Trichy .

E-mail:bhuvanarkcse@gmail.com

Mrs.G.Nalina Keerthana, She has received B.E Information Technology degree from J.J college of engineering and technology , Trichy in 2004 and ME Computer science and Engineering degree in M.I.E.T engineering college, Trichy in 2013

E-mail:roseruby1993@gmail.com

A.Rachel Roselin, She has received B.E Computer science and Engineering degree from Mount Zion college of engineering and technology, Pudukkottai in 2014 and currently pursing ME Computer science and Engineering degree in M.I.E.T engineering college, Trichy .

E-mail:roseruby1993@gmail.com