Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 41-46, 2016
ISSN 1990-9233;

DOI: 10.5829/idosi.mejsr.2016.24.TAET23318

Detection and Isolation of the Selfish Nodes Using a Collaborative Contact Based Watchdogs

T.R. Srinivasan and K.G. Chithra

Department of Computer Science and Engineering,
Vivekananda Institute of Engineering and Technology for Women, India

Abstract: Cooperation is mandatory in Mobile ad-hoc Networks (MANETs) to work properly. This Selfish node behaviour is detected when nodes do not forward the other nodes packet. This leads to overall performance degradation. One of the mechanism to detect the Selfish node is watchdogs. This mechanism is an inefficient one because it leads to a wrong detection process of false positives and a false negatives. *Sporadic contact Network such as delay tolerant Networks (DTNs), where there is a lack of enough time or* information in detecting the Selfish nodes. In such case, more advanced technique is required. We propose a collaborative approach based on the migration of the Selfish nodes awareness when a contact occurs, so that information about the Selfish nodes is quickly propagated and isolation of the Selfish node is performed in the Network.

Key words: Smart Sensing Environment, The Selfish nodes, Wireless Networks, Sensor Automation.

INTRODUCTION

In mobile Adhoc Networks, it is necessary for the receiver to receive the packet which is targeted to the particular receiver by the sender node in the Network, but this do not happen because of the presence of the Selfish node. Mobile Adhoc Network (*MANET*), has no centralized infrastructure like the base station to forward the packets to the destination and so the intermediate nodes forward [1, 2] the packet to the destination, the sender trusts the intermediate nodes for their packet delivery. The disloyal intermediate nodes are termed as the Selfish nodes. Packets are not forwarded by selfish node due to several reasons like as to save their resources and to save their energy.

Essential overall performance requires detection of such nodes in the Network. Watchdog is the one of the mechanism to detect such the Selfish nodes. When it detects the Selfish node then it is marked as positive, when it detects the nonselfish node then it is marked as negative. This is illustrated through below diagrammatic representation. Due to the presence of the Selfish nodes in the Network, there is a degradation in the throughput and the Network seems to be not a trustworthy one. Detection of the Selfish nodes only helps in moving to an alternative path for the transmission of the data, but no the Selfish node avoidance. Future work is to detect and avoid the Selfish nodes in the Network which gives an increased performance and good enhancement regarding performance and throughput. Detection of the Selfish node is illustrated in the below Figure 1.

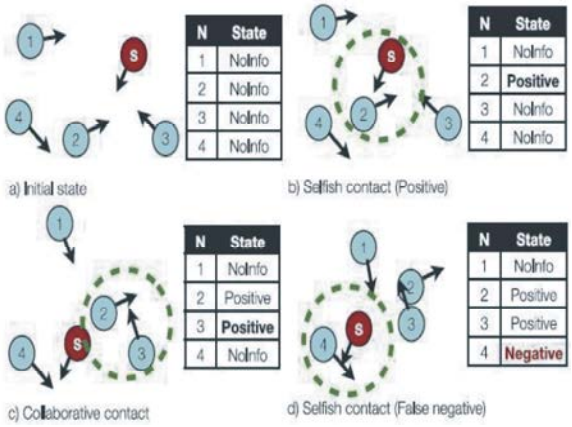

Fig. 1: Detection of the Selfish nodes

Positive represents the presence of the Selfish node in the Network while the negative represents the no the Selfishness of the node. Watchdog after marking the node either as positive or negative, it passes that information to the neighbouring nodes when it has a contact with it.

Corresponding Author: T.R. Srinivasan, Department of Computer Science and Engineering,
Vivekananda Institute of Engineering and Technology for Women, India.

This is known as the diffusion of information about the Selfish and the nonselfish nodes detection to the neighbouring nodes. In this figure there is one the Selfish node. At the starting there is no information about the Selfish nodes. Then it marks positive and negative based on the Selfishness of the intermediate node. It stores that information and later when it contacts the other node it passes that information to that node.

The diffusion of positive and negative information can produce the fast diffusion [3, 4] of wrong information and therefore, a poor Network performance. For example, in Fig. 1, on the last state (d), node 2and 3 have a positive information and node 4 has a negative information (a false negative). Now, node 1, which has no information about the Selfish node, has several possibilities: if it contacts the Selfish node it may be able to detect it; if it contacts node 2 or 3 it can get a positive information, but if it contacts node 4, it can get a false negative.

A false positive is the detection information which is actually wrong about the detected node.it is the detection of positive, when that particular node is not the Selfish node. A false negative is the detection information which is actually wrong about the detected node.it is the detection of negative, when that particular node is the Selfish node. This is the serious drawback of the watchdog mechanism and which makes it inefficient mechanism for detecting the Selfish nodes in the Network

Fig. 2 shows the functional structure of CoCoWa and their main components. The Watchdog has two functions: the Selfish node detection and the new contact detection. The events produced by the detecting node(Watchdog) about the detected nodes: positive event when the watchdog detects a the Selfish node, negative event when the watchdog detects that a node is not the Selfish and no detection event when the watchdog do not have not much information about a node (for example if the contact time is very low or it do not overhear enough messages). The new contact detection is based on neighbourhood packet overhearing; thus, when the watch-dog overhears packets from a new node it is assumed to be a new contact and so it generates an event to the Network information module. The Diffusion module has two functions: the transmissions as well as the reception of positive (and negative) detections. A key issue of our approach is the diffusion of information. The positive detections are transmitted with low overhead once the number of selfish node is low than total number of nodes. This leads to some serious demerits like a false positives can be spread over the Network very fast. Thus, the transmission of negative detections is necessary to neutralise the effect of a false positives, but sending all known negative detections can be a trouble, producing the fast diffusion of a false negatives. A negative diffusion factor is introduced which is the ratio of negative detections of actually transmitted. This Value ranges from 0 (no negative detections are trans-mitted) to 1 (all negative detections are transmitted). We will show in the evaluation section that a low Value for the factor is enough to neutralise the effect of a false positives and a false negatives. Finally, a message is transmitted with information to new neighbour node when it receives the diffusion module. Once a message is received by a node, an even is generated to Network information module with positive detection list. Update module is used to update the information. The information's of other nodes like No Info state, Positive state and Negative state are hold by the node. NO Info has no information about a node. In Positive state, node is believed as selfish. Negative state means node is believed as not selfish. Node consists of both direct and indirect information's. Fig 2

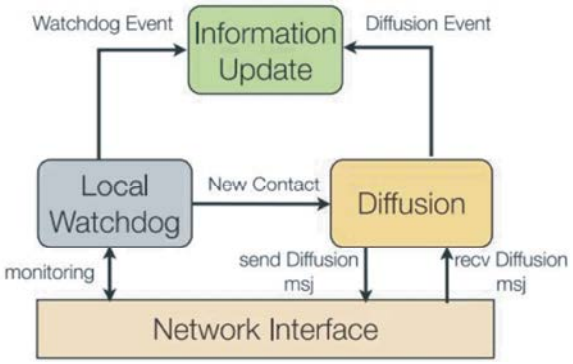

Fig. 2: watchdog mechanism

This gives the overall structure of the watchdog. Due to its wrong diffusion, we go to a new mechanism known as a collaborative watchdog which overcomes from his a false negative and a false positives.in a collaborative watchdogs. We give the IP address of the receiver and route node. Route node is the node through which the packet reaches the destination. We can say the intermediate node which forward the packet is the route node. We also specify the file which has to reach the destination. A collaborative watchdog is the contact based. When it contacts the neighbouring node it passes the detection information to that neighbouring node. When the route node is the Selfish node then the watchdog sends the acknowledgement to the sender.

Acknowledgement message is the text display of "resend the file to any other route as this chosen route is a the Selfish node". After receiving such acknowledgement, the sender chooses the different route to transmit its file and checks for any acknowledgement about the Selfish node, if it do not receive any acknowledgement to some period it confirms that its text file reached the destination successfully.

A collaborative watchdog has the route details and detected details in their storage. The storage here we use is a database created in MYSQL and retrieving that information through query language like a select statement. It detects the Selfish node through file size. If the send file size changes during transmission of file through the route, it [5] detects that route node as the Selfish route node and if the send file and transmitting file size are equal then the file packet reaches the destination and stores the information about sender IP address and the route node Ip address through which the file forwarded to the destination and the respective receiver node to which the file has reached finally.

When new neighbouring node contacts the previous sender node, it transmits the information that is available with it about the Selfishness of the nodes in the Network.

Architecture and Dataflow Diagram Overview

System Architecture:

The Network is modeled as
(N = C+M+S).

where

- N is wireless mobile nodes
- C is a collaborative nodes
- M is malicious nodes
- S is the Selfish nodes

MANETs assumes that mobile nodes voluntary cooperate to work properly. This cooperation is a cost intensive activity and some nodes can refuse to cooperate, leading to the Selfish node behaviour where sometimes watchdogs lack of enough time or information to detect the Selfish nodes. Thus, we propose a collaborative contact-based watchdog (CoCoWa) as a collaborative approach based on the diffusion of local the Selfish nodes awareness when a contact occurs, so that information about the Selfish nodes is quickly propagated. As shown in the paper, a collaborative approach reduces the time and increases the precision when detecting the Selfish nodes.

The local watchdog is modeled using mainly and importantly with the three parameters which give detection mechanism three parameters: the probability of detection pd, the ratio of a false positives pfp and the ratio of a false negatives pfn. The first parameter, the probability of detection (pd), reflects the probability that, when a node contacts another node, the watchdog has enough information to generate a PosEvt or NegEvt event. This Value depends on the effectiveness of the watchdog, the traffic load and the mobility pattern of nodes. For example, for opportunistic Networks or DTNs [6] where the contact are sporadic and have low duration, this Value is lower than for MANETs. Furthermore, the watchdog can generate false positives and false negatives. A false positive is when the watchdog generates a positive detection for a node that is not the Selfish node.

In our architecture we monitor the nodes in the Network which behave normally and the malicious nodes [7] which are disloyal and alter any content in the file and sends that file to the destined receiver and the Selfish nodes which do not forward the packets due to its the Selfishness of saving its own resources. The monitoring mechanism used here is COCOWA MECHANISM which monitors all such nodes in the Network and reports to the sender of misbehaviour [8] through acknowledgement as soon as the sender receives the ACK(acknowledgement) from the cocowa. It has to re_route to the different path which increases the precision when detecting the Selfish nodes.

We propose a collaborative contact-based watchdog (CoCoWa) as a collaborative approach based on the diffusion of local the Selfish nodes awareness when a contact occurs, so that information about the Selfish nodes is quickly propagated. As shown in the paper, A collaborative approach reduces the time and increases the precision when detecting the Selfish nodes. MANET is a mobile Adhoc Network which is an infrastructure less Network without the presence of any centralized co-ordinator like the base station. Example for infrastructure based Network is cellular based Network in which the mobile node contacts the base station to forward the packets to the other nodes. Incase of mobile Adhoc Network the intermediate nodes present in between any sender and receiver forward the packet to the required destination without the requirement of the base station. In such a Network COCOWA is the best mechanism in the Selfish node detection where the Selfish node is intermediator nodes which forward the packet. Based on the file size the detection is performed which gives an

accurate detection of the Selfish nodes avoiding both a false positive and a false negatives. Precision or accuracy is the main advantage if the Collaborative Contact Based Watchdog technique. This has been a serious disadvantage earlier which is overcome by this efficient technique COCOWA.

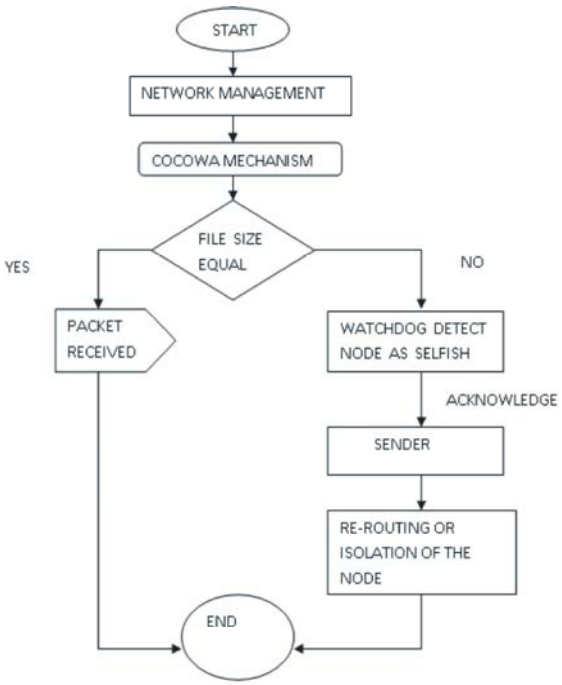

Fig. 3: Dataflow diagram of System Architecture

Malicious Nodes and Attacker Model: Malicious nodes attacks the CoCoWa system with wrong information generation about the nodes. Thus, the attacker model addresses the behavior or capabilities [9, 10] of these malicious nodes. A malicious node attack consists of trying to send a positive about a node that is not a the Selfish node, or a negative about a the Selfish node, with the goal of producing a false positives and a false negatives on the rest of nodes. To follow this procedure, working knowledge of CoCoWa is must. This behaviours effectiveness depends on the rate and precision that malicious nodes can generate wrong information.

Malicious nodes are assumed to have communications hardware similar to the rest of nodes so that they can hear all neighbor messages in a similar range. The attacker used high-gain antennas to increase its communications range. False information are distributed in a more effective manner. Regarding the diffusion of information on the Network, proposed approach do not assume any security measures, such as message ciphering or node authorization

Nevertheless, if these measures exist, the effect of malicious nodes in CoCoWa is reduced or even non-existent. The diffusion module accepts messages from every node, even it is from a malicious ones. Thus, malicious nodes [5] are assumed to be active and use this information to generate wrong positives/negatives about other nodes. Nevertheless, we assume that malicious nodes cannot impersonate other nodes and do not collude with other malicious nodes (that is, they do not cooperate [11] with them).

Detection of the Selfish Nodes: In this section we introduce an analytical model for evaluating the performance of CoCoWa. The goal is to obtain the detection time (and overhead) of the Selfish node in a Network. This model takes into account the effect of a false negatives. A false positives do not affect the detection time of the Selfish node, so pfp is not introduced in this model. The purpose of this division is to obtain analytically the time [12] and the overhead required for the subset of destination nodes to detect the Selfish node.

Pseudocode:

```
READ X,Y;
SET ORG_SIZE=X;
IF(Y<X||Y>X)
ACK=CORRUPTED;
WRITE ACK;
READ ACK;
SET ROUTENODE=ALTERNATE IP;
SET X=FILE.TXT;
WRITE X;
```

Two variables namely X and Y are declared. X is set to original file size and Y is set to forwarded file size. If the forwarded file size is less than or greater than the original file size ‘X’ then Y is said to be corrupted and the forwarded node is marked as the Selfish node. Acknowledgement about Selfishness of the forwarded node is sent to the sender. When the sender reads the acknowledgement it marks the forwarded node as the Selfish node, then it performs the re_routing. Re_routing is done by sending the same file in the alternate path which is different from the previously selected path. The Selfish node list is stored in the database and when other nodes contact it, it sends the stored information to the contact node. This process is known as diffusion of the Selfishness information.

The alternate path may or may not contain the Selfish node. If it do not contain any the Selfish node in the path, it forward the packet to the correct destination. If it is the Selfish node the another alternate path is selected for sending the packet to the destination.

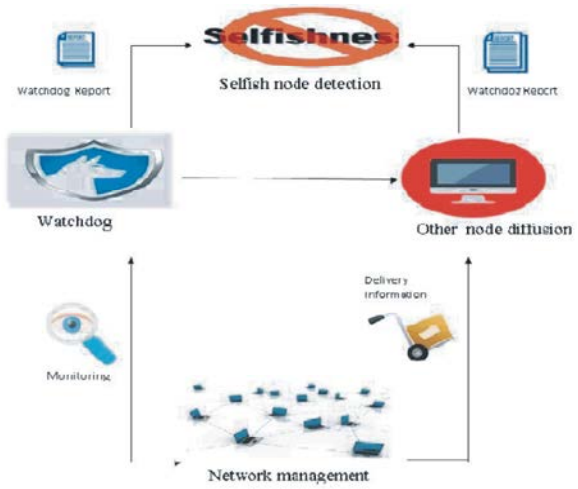

Fig. 4: Architecture diagram

Packets Re-routing: Routing is the process of selecting best paths in a Network. Early days, routing meant forwarding Network traffic between Networks. Routing is performed for different Networks such as the telephone Network (circuit switching), electronic data Networks (like Internet) and transportation Networks. Proposed method mainly concentrate on routing in electronic data Networks with packet switching technology.

Packet switching Network's routing process is to direct the transit of logically addressed Network packets from their source toward their ultimate destination through intermediate nodes while the Intermediate nodes are typically Network hardware devices like routers, bridges, gateways, firewalls, or switches. General-purpose computers forward packets and perform routing, though they are not specialized hardware and suffers from limited performance [13]. The routing process usually directs forwarding by routing tables, maintain a route's record to various Network destinations. Routing tables are constructed and held in router's memory which is efficient for routing. Mostly routing algorithms use one Network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

A model is evaluated for evaluating the effect of false positives which evaluates how fast a false positive spreads in the Network. A greater diffusion time stands for a lower impact of false positives. The diffusion time is similar to the detection time of true positives. By following the same process that in the previous model fo false negatives [8], We can derive expressions similar, for the case of a false positives. In this case, RfP represents the rate of false positive and it is derived in a similar way: Thus, the overall detection evaluates the performance of the entire Network, while the individual detection evaluates the performance.

Re_Routing is sending the file or packet destined to the receiver through alternate path when that path or route behave as the Selfish route. This the Selfish node is detected through the cocowa mechanism which efficiently detects the Selfishness by comparing the file sizes. When the send file size is not equivalent to moving packet then mechanism decides this as the misbehaving [14] route node since the size of the file or increased or decreased than original Re_Routing changes the route node and transmits the packet through that path. In every node, the watchdog mechanism works in the background and stores the positive and negative detection of the Selfishness in the routing path. The already stored information about another node behaviour is transmitted when that route node contact the sender node. Re_routing plays an important role in the correct delivery of information to the receiver without changing the content of the file. This gives the security and confidentiality of the information transmission in the mobile ADHOC Network where cooperation plays an important role in packet forwarding.

Future Work: In future work, we are giving the advancement of proposed work. When the route node misbehaves then when that route node acts as a sender, it can send its packet to other nodes and the other node forward that packet. This is in the proposed one. In future work when the Selfish route node misbehaves it cannot send its packet as sender thus, it has no other way to go. Hence it will transmit the packet correctly and loyalty. This improvement makes efficient routing and no re_routing is required.

Since the sender cannot send its file, if it do not forward other node packets.it will willingly try to forward other nodes packet to send its own file. This avoids RE-ROUTING completely and thus there is a reduce in the overall complexity of the system. This gives an improved performance in computer Networks.

CONCLUSION

We propose the collaborative contact based technique to detect the Selfish node accurately and

without delay using file size. Thus it increases the precision and time of detection. CoCoWa as collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting the Selfish nodes, reducing the harmful effect of a false positives, A false negatives and malicious nodes. CoCoWa is based on the diffusion of the known positive and negative detections. When a contact occurs between the two collaborative nodes, the diffusion module transmits and processes the positive (and negative) detections. It isolates the Selfish node in the Network as well as to improve the performance.

ACKNOWLEDGMENT

This research was supported by my Head of the Department, Prof.T.R.Srinivasan. I thank Mr.Chandra Mohan for assistance with a technique and Mr.Sathish for comments that greatly improved the manuscript.We thank famous persons Dr.Karunanithi and Dr.K.C.K.Vijaykumar, for sharing their pearls of wisdom with us during this research and we thank Mrs.E.Menaka and Mr.R.Rajagopal reviewers for their so-called insights. Mrs.Leema Mathayi helped with some technical stuff. We are also immensely grateful to my family for their comments and support, although any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

1. Buchegger, S. and J.Y. Le Boudee, 2005. Self-policing mobile ad hoc Networks by reputation systems, IEEE Commun. Mag., 43(7): 101-107.
2. Butty an, L. and J.P. Hubaux, 2000. Enforcing service availability in mobile ad-hoc WANs, in Proc. 1st Annu. Workshop Mobile Ad Hoc Netw. Comput., pp: 87-96.
3. Cai, H. and D.Y. Eun, XXXX. Crossing over the bounded domain: From exponential to power-law intermeeting time in mobile ad hoc Networks," IEEE/ACM Trans. Netw., 17(5): 1578159.
4. Douceur, J.R., 2002. The sybil attack, in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., pp: 251-260.
5. Butty an, L. and J.P. Hubaux, 2003. Stimulating cooperation in self- organizing mobile ad hoc Networks, Mobile Netw. Appl., 8: 579-592.
6. Hern andez-Orallo, E., M.D. Serrat Olmos, J.C. Cano, C.T. Calafate and P. Manzoni, 2012. Evaluation of collaborative the Selfish node detection in MANETS and DTNs, in Proc. 15th ACM Int. Conf. Modeling, Anal. Simul. Wireless Mobile Syst., New York, NY, USA, pp: 159-166.
7. Abbas, S., M. Merabti, D. Llewellyn-Jones and K. Kifayat, 2013. Lightweight sybil attack detection in manets, IEEE Syst. J., 7(2): 236-248.
8. Hollick, M., J. Schmitt, C. Seipl and R. Steinmetz, 2004. On the effect of node misbehavior in ad hoc Networks, in Proc. IEEE Int. Conf. Commun., pp: 3759-3763.
9. Gao, W., Q. Li, B. Zhao and G. Cao, 2009. Multicasting in delay tolerant Networks: A social Network perspective, in Proc. 10th ACM Int. Symp.Mobile Ad Hoc Netw. Comput., pp: 299-308.
10. Groenevelt, R., P. Nain and G. Koole, 2005. The message delay in mobile ad hoc Networks, Perform. Eval., 62: 210-228.
11. Bansal, S. and M. Baker, 2003. "Observation-based cooperation enforcement in ad hoc Networks" arXiv:cs.NI/0307012, 2003.
12. Hern andez-Orallo, E., M.D. Serrat, J.C. Cano, C.M.T. Calafate and P. Manzoni, 2012. Improving the Selfish node detection in MANETs using a collaborative watchdog, IEEE Comm. Lett., 16(5): 642-645.
13. Hortelano, J., J.C. Cano, C.T. Calafate, M. de Leoni, P. Manzoni and M. Mecella, 2010. Black hole attacks in p2p mobile Networks dis-covered through Bayesian filters, in Proc. Int. Conf. Move Meaningful Internet Syst., pp: 543-552.
14. Rajan, C. and N. Shanthi, 2013. Misbehaving attack mitigation technique for multicast security in mobile ad hoc Networks (MANET). Journal of Theoretical and Applied Information Technology, 48(3): 1349-1357.