Handling Selfishness over Collaborative Mechanism in a Mobile Ad hoc Network

K. Anish Pon Yamini[1,*], Suthendran Kannan[2] and Arivoli Thangadurai[3]

[1]*Research Scholar, Department of Electronics and Communication, Kalasalingam Academy of Research and Education, Krishnankoil - 626 126, Tamilnadu, India*
[2]*Associate Professor, Department of Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil - 626126, Tamilnadu, India*
[3]*Senior Professor, Dept of Electronics and Communication, Karpagam College of Engineering, Coimbatore - 641032, Tamilnadu, India*
E-mail: anish.yamini@gmail.com; k.suthendran@klu.ac.in; t.arivoli@gmail.com
**Corresponding Author*

Received 13 February 2018; Accepted 24 March 2018;
Publication 16 April 2018

Abstract

Major constraint of Mobile ad hoc networks is unpredictable mobility and limited resources like energy consumption which may ultimately end in failure of network connectivity and performance deterioration. Almost all of the suggested techniques presume that every nodes share their memory space with full collaboration. But in realism, few nodes selfishly decide either to cooperate partially only with other nodes, or not at all. Thus, a advanced collaborative mechanism based on dissemination of selfish node awareness is suggested. Numerical results reveal that such mechanism results in better improvement in performance.

Keywords: Adhoc networks, Replication techniques, collaborative mechanism, Detection.

Journal of Cyber Security, Vol. 7_1, 39–52.
doi: 10.13052/jcsm2245-1439.714

1 Introduction

A key concern in Mobile Ad Hoc networks are networks which self organize themselves and have no central coordination point. Physical reachability within nodes is a necessary criterion for communication. Each node has to meet higher complexity as every node has to implement routing procedure. Nodes mobility creates frequent topological fluidity; nodes join, leave or rejoin the network often. Dynamic node reconfigurations are authorized for network connectivity. A latest emerging network design currently receiving significant attention is COOPERATIVE networking which provides cost-effective services and applications.

In Mobile ad-hoc networks (MANETs) direct communications between mobile nodes are possible if they are within communication range. For mobile nodes to support cooperation which is a cost demanding activity makes a node to have a selfish behaviour. Selfishness can be explained as nodes refusing or unwilling to forward packets to other nodes inorder to salvage their resources. Two main strategies suggested in literatures are a) incentive or motivation based approaches, and b) detection and exclusion [2] based approaches. First model motivates nodes for active participation in the forwarding activities. Second model is a genuine way to handle selfish nodes.

In CoCoWa, the main goal is detection of selfish nodes and no attempt to incentivize selfish nodes participation or to exclude them was made. A positive detection is marked if the selfish node is detected by watchdog if not a negative detection is marked. There is a greater chance of watchdogs to fail on this detection. Such a scenario ends in creating false positives and false negatives which vigorously decline performance. Existence of malicious nodes is a major concern for cooperative approaches. Under such instance, results can be more adverse. Suppose consider that if any one node behaves dishonesty regarding the status of another, results in a rapid dissemination of false negatives or false positives. Detection of malicious nodes using watchdogs, which intentionally participate in network communication by hiding their behaviour from the network, is a great challenge. As we often assume the presence of malicious nodes we are supposed to evaluate their influence on the network. In this proposed scheme a new Collaborative Contact-based Watchdog was introduced that effectively blends local watchdog detection and then disseminating the report throughout the network. By this approach, nodes can soon have better knowledge about the nodes which are selfish rapidly. Our intense objective is detection time reduction and thereby achieving high fidelity by introducing certain degree of collaboration on their watchdog schemes.

Several issues are introduced due to the dissemination of positive or negative detections of selfish nodes. First of this is the information consolidation which deals with the reliability about neighbor's positive and negative detections, especially when there is a mismatch with the local watchdog detection.

An analytical performance model was designed where our network is modeled as a continuous time Markov chain (CTMC) and expressions are derived for attaining the time and over-head cost of selfish nodes detection under the influence of false positives, false negatives and malicious nodes.

Our experiment reveals a considerable time reduction required for detecting selfish nodes when the performance of the CoCoWa is compared with a traditional watchdog. Furthermore a great minimization on the effect of false negatives and false positives is achieved and reputation detection scheme reduces the pernicious effect of malicious nodes. Our evaluation is done based on real mobility scenarios.

2 Architecture Overview

In general, a selfish node denies packet relaying to safeguard its owned assets. This particular behavior indicates that the selfish nodes do not participate in routing or relay data packets. Network monitoring using local watchdogs technique are employed to detect this selfish behavior is. A node's watch dog overhears the neighbor's packets transmission and reception to detect deviation between received to re-transmitted packets ratio. Based on this, the local watchdog decides to generate a positive detection if it finds a node to be selfish or a negative detection if not.

An outline of CoCoWa architecture which is the fusion of a local watchdog and the information dissemination is shown in Figure 1. Initially assume a single selfish node and all the other nodes are unaware of this selfish node. Using its watchdog, a node has the ability to find a selfish node and mark it as a positive detection or a negative if not. This information is relayed to the other nodes when this node contacts some other node within its communication range, now both the nodes share the knowledge about these positive or negative detections. Overall, by using watchdog direct awareness about selfish nodes or indirect awareness provided by its neighbors through the collaborative transmission of information can be achieved.

Three main components of CoCoWa are shown in Figure 2

- Local watchdog
- Diffusion module
- Information update

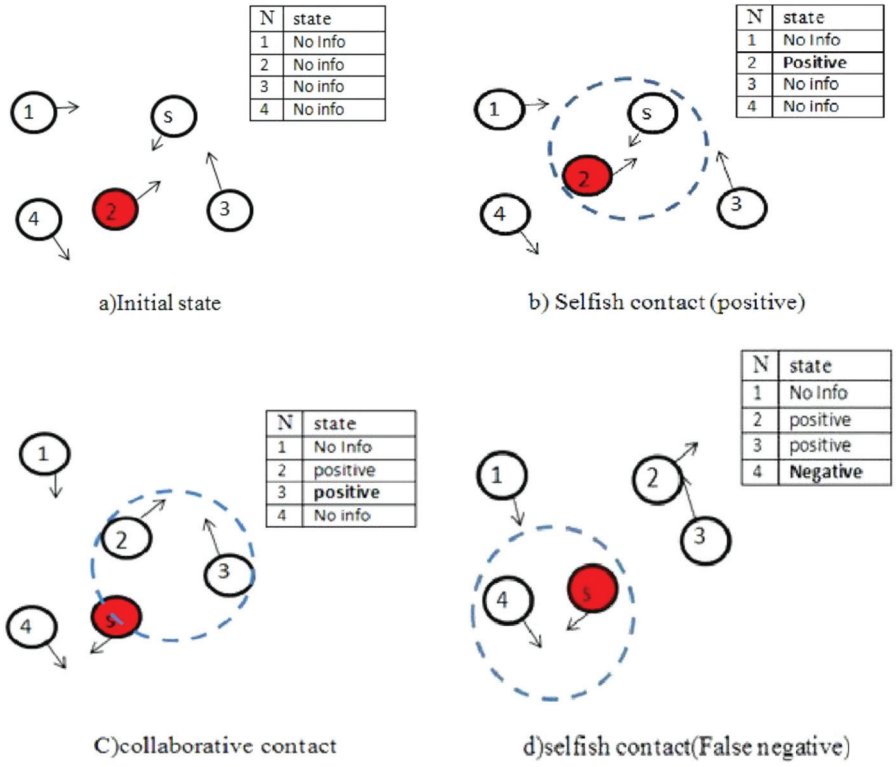

Figure 1 An example illustrating collaborative mechanism.

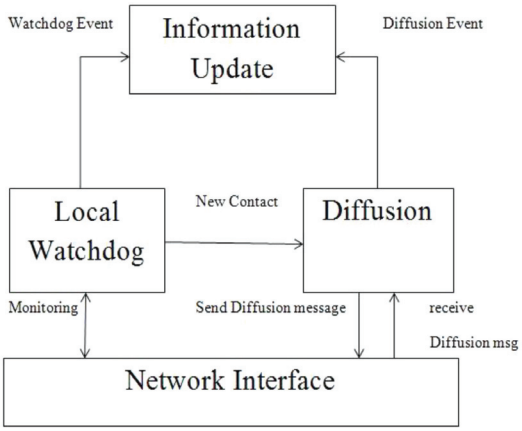

Figure 2 Collaborative mechanism architecture.

1. Local watchdog:

Two of its main functions are,

- Selfish node detection
- New contact detection

The events generated by the local watchdog about neighbor nodes are POSEVT(Positive event), NEGEVT(Negative event).

Diffusion module:

Two functions of Diffusion module are,

- Transmission of detection
- Reception of detection

Only very few selfish nodes exists. So less overhead are required while transmitting positive detections.

2. Information update:

Two functions of information update module are,

- Updating information
- Consolidating the information

Internal information maintained by a node regarding other nodes:

- NOINFO state
- POSITIVE state
- NEGATIVE state

3 System Model

Figure 3 presents the flowchart of the proposed selfish node detection algorithm CoCoWa. We model the network consisting of a group of N mobile nodes with Co collaborative nodes, M malicious nodes and SF selfish nodes (N=Co+M+SF). The total control messages transmitted denotes overhead. The overhead time required to expose the selfish nodes throughout the network can be attained.

Assume that there are non cooperative selfish nodes in the network. So the impact of each selfish node has to be analyzed individually. Also consider the case where a greater no of selfish nodes (SF>1) exists on a network with N nodes, cooperative nodes C = N-SF. Then information $_{\mathrm{target-node}}$ will be compared to the information $_{\mathrm{neighboring-node.}}$ For example N = 8 & information $_{\mathrm{target-node}}$ is 6. then 8>6, so the target node is identified as a

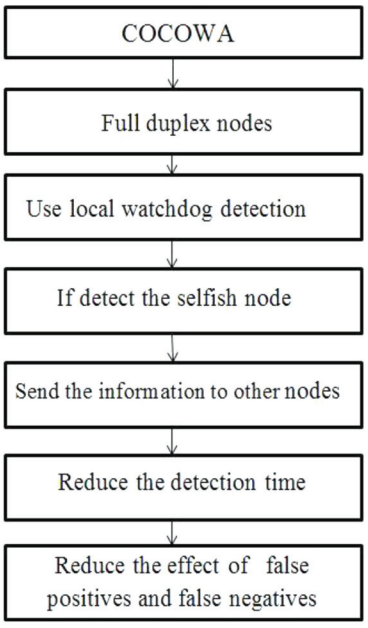

Figure 3 Selfish node detection algorithm.

selfish node. Local watchdog and diffusion modules provide the states of the nodes as PosEvt or NegEvt and so CoCoWa is event driven. A new value called reputation value ρ is updated by these events using the expression:

$$\rho = \rho + \Delta \; \Delta = \begin{cases} +\delta \quad (\text{PosEvt, Local}) \\ +1 \; (\text{PosEvt, Indirect}) \\ -\delta \quad (\text{NegEvt, Local}) \\ -1 \; (\text{NegEvt, Indirect}) \end{cases} \quad \delta \geq 1$$

where δ is the margin. Normally ρ is incremented for PosEvt event and decremented for a NegEvt event. Threshold value is represented as θ. A nodes state shift between Positive ($\rho \geq \theta$), and Negative ($\rho \leq -\theta$). Else, it is set as NoInfo state which means that it bears no information about a node's selfishness. Dynamic behaviour and flexibility increases with the combination of δ and θ parameters. As an example assume $\theta = 2$ and $\delta = 1$ represents that minimum a local and an indirect event is required for changing the state. Indirect and local watchdog information is trusted more in our proposed approach. Also wrong local decisions are compensated.

Updating strategies are twofold. First, fast dissemination of false positive and false negatives are reduced by setting the threshold θ which otherwise increases detection delay. Second, the most recent information is considered for the decision about a selfish node. Suppose, previously a node may be marked as positive state and later after receiving several NegEvt from other nodes the Negative state is updated. All the state informations are associated with an expiration timer. It's a straight-forward implementation mechanism. All the received events are marked with a time stamp, an opposite event is generated once the timer expires.

4 Performance Analysis

Performance estimations are discussed in this section.

A. Scenario setting
The NS2 simulator is used to simulate the performance of the proposed protocol where 5 to 25 nodes are randomly distributed two dimensional square region 1000×1000 m^2 areas. Quantitative metrics used for the performance evaluation are detection rate, throughput, and packet delivery ratio. The node density is considered as the variable parameter. Here the proposed algorithm is compared with the local watchdog approach. The discussion about the performance metrics are given below.

B. Performance parameters
Detection rate: The detection rate analysis the impact on the collaboration grade over the capability of CoCoWa. Significant improvements in network performance are produced if timely actions are taken to avoid the selfish node which in turn reduces the detection time considerably from hours to seconds.

Throughput: Average rate of successful data packets (in bit per second) received at destination node over a communication channel. This metric reflects the channel utilization. Various factors affecting network throughput are end-user behaviour, available processing power of the system components, the limitations of underlying analog physical medium.

Packet delivery ratio: Ratio between the total numbers of data packets delivered successfully at destination node to total number of data packets generated by the source. Higher value of packet delivery ratio refers to the protocol consistency.

The graph for number of packets vs. node density is shown in Figure 4. $\mathrm{P_{fn}} = \mathrm{P_{fp}} = \mathrm{M} = \mathrm{P_m} = 0$ means there are no false positives, negatives or malicious nodes. Simulation results illustrate an improved performance

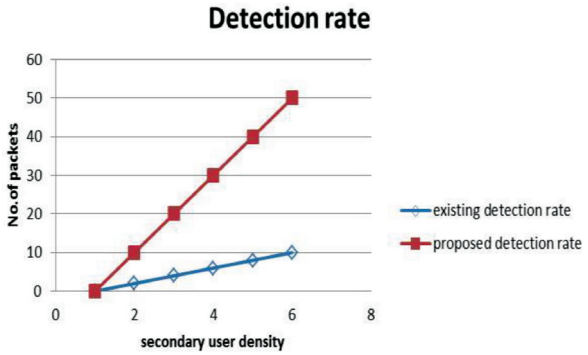

Figure 4 Number of packets v/s user density.

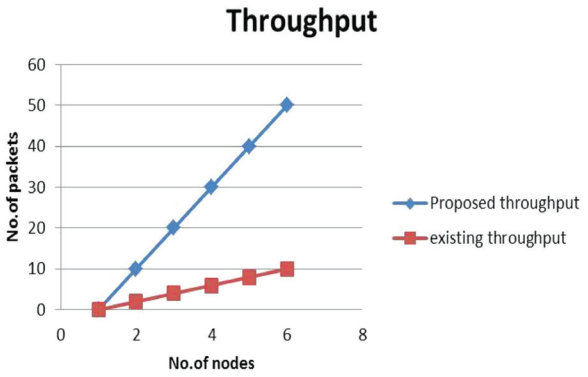

Figure 5 Number of packets v/s nodes.

evaluation. This is because only positive detections are transmitted also in this experiment the local watchdog is estimated.

The throughput is shown in the Figure 5. Simulation result illustrates an improved throughput. Evenly it proves the fact that more PDR increases throughput. This shows that target reachabilty is high in our algorithm without reducing the quality of delivered packets.

The graph for packet delivery ratio is shown in the Figure 6, simulation results illustrate an improved packet delivery ratio this is because, proposed approach merges local watchdog detections and disseminates information over the network.

The graph for Overhead vs node density is shown in the Figure 7. Our proposed approach have a small overhead, because of which we are able to identify selfish nodes, propagate reputation, and take necessary actions depending on the severity of their misbehaviour. The graph shows that the

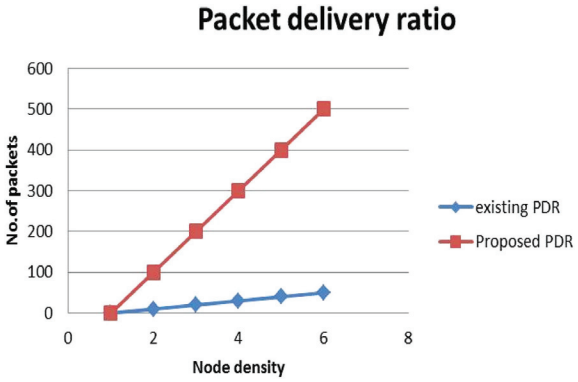

Figure 6 Number of packet v/s node density.

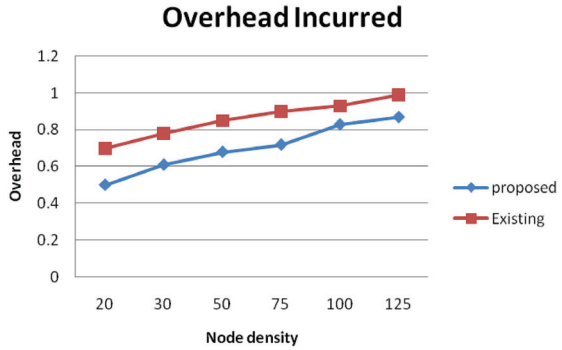

Figure 7 Overhead vs Node density.

overhead increases with the node density because higher the nodes higher the events which eventually results in higher overhead.

5 Conclusion

Our paper aims to identify the impact of CoCoWa as a collaborative contact-based watchdog. The result analysis reveals that there is a remarkable reduction from the harmful effect of false positives, false negatives and malicious nodes. We can even improve throughput and reduce detection time. We plan to use cluster-based selfish node identification with encounter/game theory algorithm, keeping these trade-offs in mind. CoCoWa due to its improved the effectiveness of detecting selfish nodes can be employed in energy constrained applications.

References

[1] Abbas, S., Merabti, M., Llewellyn-Jones, D., and Kifayat, K. (2013). Lightweight sybil attack detection in manets. *IEEE Systems Journal*, *7*(2), 236–248.

[2] Zhang, D., Song, H., and Yu, L. (2017). Robust fuzzy-model-based filtering for nonlinear cyber-physical systems with multiple stochastic incomplete measurements. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *47*(8), 1826–1838.

[3] AbdelMohsen, D., and Abdelkader, T. (2015). Detecting selfish nodes and motivating cooperation in Mobile Ad-hoc Networks. In *Tenth International Conference on Computer Engineering & Systems (ICCES)*, 301–306.

[4] Hlavacek, D. T., and Chang, J. M. (2015), Design and Analysis of a Method for Synoptic Level Network Intrusion Detection. In *IEEE 39th Annual Computer Software and Applications Conference (COMPSAC)*, 2, 516–524.

[5] Eidenbenz, S., Resta, G., and Santi, P. (2008). The COMMIT protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes. *IEEE Transactions on Mobile Computing*, *7*(1), 19–33.

[6] Hernandez-Orallo, E., Olmos, M. D. S., Cano, J. C., Calafate, C. T., and Manzoni, P. (2015). CoCoWa: A collaborative contact-based watchdog for detecting selfish nodes. *IEEE Transactions on Mobile Computing*, *14*(6), 1162–1175.

[7] Hernandez-Orallo, E., Serrat, M. D., Cano, J. C., Calafate, C. T., and Manzoni, P. (2012). Improving selfish node detection in MANETs using a collaborative watchdog. *IEEE Communications Letters*, *16*(5), 642–645.

[8] Keerthika, V., and Suganthe, R. C. (2013). Watchdog: Reduce time delay for spreading selfish information in manet. In *International Conference on Information Communication and Embedded Systems (ICICES)*, 1104–1107.

[9] Raz, N. R., and Akbarzadeh-T, M. R. (2013). Cooperation Tuning in MANETs: A fuzzy approach Fuzzy behaviors of node in the presence of conflict. In *13th Iranian Conference on Fuzzy Systems (IFSC)*, 1–6.

[10] Passarella, A., and Conti, M. (2011). Characterising aggregate inter-contact times in heterogeneous opportunistic networks. In *International Conference on Research in Networking,* 301–313. Springer, Berlin, Heidelberg.

[11] Paul, K., and Westhoff, D. (2002). Context aware detection of selfish nodes in dsr based ad-hoc networks. In *Proceedings of the Vehicular Technology Conference, VTC 2002-Fall.* 4, 2424–2429.
[12] Rout, S.. Turuk, A. K., and Sahoo, B. (2009). "Energy Efficiency in Wireless Ad hoc Network using Clustering", in *proceedings on 12th International Conference on Information Technology*, 223–226.
[13] Sengathir, J., Manoharan, R., and Kumar, R. R. (2013). Markovian process based reputation mechanisms for detecting selfish nodes in MANETs: A survey. In *Fifth International Conference on Advanced Computing (ICoAC)*, 217–222.
[14] Gupta, S., Nagpal, C. K., and Singla, C. (2011). Impact of selfish node concentration in MANETs. *International Journal of Wireless & Mobile Networks (IJWMN)*, 3, 29–37.
[15] Toh, C. K. (1997). Associativity-based routing for ad hoc mobile networks. *Wireless Personal Communications*, *4*(2), 103–139.
[16] Zhu, H., Fu, L., Xue, G., Zhu, Y., Li, M., and Ni, L. M. (2010). Recognizing exponential inter-contact time in VANETs. In *Proceedings in the INFOCOM,* 1–5.
[17] Wireless Communications: Principles and Practice. *Theodore S. Rappaport*. Prentice Hall, 2nd edition, December 2001.
[18] Network Simulator 2 (ns2). Available at: http://www.isi.edu/nsnam/ns/

Biographies

K. Anish Pon Yamini is a Research Scholar in the Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India, from 2012. She gained Master's degree in Communication System from SRM institute of Science and Technology in 2005. She joined in the Department of Electronics and Communication

Engineering at Arunachala College of Engineering for Women, Kanyakumari as a Assistant Professor in 2012. Her teaching and research interests include Computer networks, Wireless Networks, Mobile Computing. She is actively involved in research activities in the field of adhoc wireless networks.

Suthendran Kannan received his B.E. Electronics and Communication Engineering from Madurai Kamaraj University in 2002; his M.E. Communication Systems from Anna University in 2006 and his Ph.D Electronics and Communication Engineering from Kalasalingam University in 2015. He was a Research and Development Engineer at Matrixview Technologies Private Limited, Chennai for a couple of years. He is now the Head, Cyber Forensics Research Laboratory and Associate Professor in Information Technology, Kalasalingam Academy of Research and Education. His current research interests include Cyber Security, Communication System, Signal Processing, Image Processing, etc.

Arivoli Thangadurai completed his M.Sc. in 1978 in The American College, Madurai. Then he did his research in the field of Solid State Devices, and received M.Sc(Engg) and Ph.D. degrees in 1982 and 1987 respectively from Electrical and Communication Engineering Department of Indian Institute of

Science, Bangalore. He has worked as an ASIC designer in India and Australia for more than 15 years. He has contributed to more than 5 successful tape-outs, which include the world's first WLAN base band processor in Radiata, Australia. Currently, he is working as a Senior Professor in ECE department in Karpagam College of Engineering, India. His areas of interest include Electronic Devices, VLSI Design and Wireless Communication Systems.